DOCKET NO.: 267285US90PCT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Yusuke HISADA, et al.
SERIAL NO.: NEW U.S. PCT APPLICATION
FILED: HEREWITH
INTERNATIONAL APPLICATION NO.: PCT/JP04/09446
INTERNATIONAL FILING DATE: July 2, 2004
FOR: REMOTE-ACCESS VPN MEDIATING METHOD AND APPARATUS

REQUEST FOR PRIORITY UNDER 35 U.S.C. 119 AND THE INTERNATIONAL CONVENTION

Commissioner for Patents
Alexandria, Virginia 22313

Sir:

In the matter of the above-identified application for patent, notice is hereby given that the applicant claims as priority:

COUNTRY	APPLICATION NO	DAY/MONTH/YEAR
Japan	2003-271202	04 July 2003

Certified copies of the corresponding Convention application(s) were submitted to the International Bureau in PCT Application No. PCT/JP04/09446. Receipt of the certified copy(s) by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

Respectfully submitted,
OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Masayasu Mori
Attorney of Record
Registration No. 47,301
Surinder Sachar
Registration No. 34,423

Customer Number
22850

(703) 413-3000
Fax No. (703) 413-2220
(OSMMN 08/03)

PCT/JP2004/009446

日本国特許庁
JAPAN PATENT OFFICE

28.07.2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年 ７月 ４日

出願番号
Application Number: 特願２００３－２７１２０２
[ST. 10/C]: [ＪＰ２００３－２７１２０２]

出願人
Applicant(s): 日本電信電話株式会社

２００４年 ９月 ２日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号 出証特２００４－３０７８７４１

【書類名】　特許願
【整理番号】　NTTH147644
【提出日】　平成15年 7月 4日
【あて先】　特許庁長官　殿
【国際特許分類】　G06F 17/00
【発明者】
　【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
　【氏名】　久田　裕介
【発明者】
　【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
　【氏名】　鶴岡　行雄
【発明者】
　【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
　【氏名】　小野　諭
【特許出願人】
　【識別番号】　000004226
　【氏名又は名称】　日本電信電話株式会社
　【代表者】　和田　紀夫
【代理人】
　【識別番号】　100073760
　【弁理士】
　【氏名又は名称】　鈴木　誠
【手数料の表示】
　【予納台帳番号】　011800
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1

【書類名】特許請求の範囲
【請求項１】
ＩＰネットワークにＶＰＮクライアント装置及びＶＰＮゲートウェイ装置が接続され、ＶＰＮゲートウェイ装置により管理されるローカルエリアネットワークに通信装置が接続され、前記ＩＰネットワークに接続された任意のＶＰＮクライアント装置と、ＶＰＮゲートウェイ装置、及び、ＶＰＮゲートウェイ装置に管理されるローカルエリアネットワークに接続された任意の通信装置との間のトンネリングプロトコルによるリモートアクセスＶＰＮを実行するシステムにおけるリモートアクセスＶＰＮ仲介方法であって、
前記ＩＰネットワーク上に仲介装置を設け、前記ＶＰＮゲートウェイ装置から前記通信装置に割り当てられたプライベートＩＰアドレスを示す情報（以下、アクセスコントロールリスト）を前記仲介装置に送信し、該仲介装置で記憶することを特徴とするリモートアクセスＶＰＮ仲介方法。
【請求項２】
前記仲介装置と前記ＶＰＮゲートウェイ装置との間の通信路を暗号化して、前記ＶＰＮゲートウェイ装置からアクセスコントロールリストを前記仲介装置に送信することを特徴とする請求項１記載のリモートアクセスＶＰＮ仲介方法。
【請求項３】
前記仲介装置は、前記ＶＰＮゲートウェイ装置を認証し、認証に成功した場合に、前記ＶＰＮゲートウェイ装置により送信されたアクセスコントロールリストを記憶することを特徴とする請求項１もしくは２記載のリモートアクセスＶＰＮ仲介方法。
【請求項４】
前記仲介装置は、前記ＶＰＮクライアント装置から前記ＶＰＮゲートウェイ装置に割り当てられたＩＰアドレスの検索要求を受信したなら、前記ＶＰＮクライアント装置が前記ＶＰＮゲートウェイ装置のアクセス権限を有するかどうか検証し、アクセス権限を有する場合に限り、
（１）アクセスコントロールリストを参照して、通信装置に割り当てられたプライベートＩＰアドレスを取得し、
（２）ドメインネームサーバを検索してＶＰＮゲートウェイ装置に割り当てられたＩＰアドレスを取得し、
（３）ＶＰＮクライアント装置とＶＰＮゲートウェイ装置との間の認証に用いる共通鍵を生成し、
（４）仲介装置とＶＰＮクライアント装置との通信路を暗号化して、ＶＰＮゲートウェイ装置のＩＰアドレス、通信装置のプライベートＩＰアドレス及び共通鍵をＶＰＮクライアント装置に送信し、
（５）　仲介装置とＶＰＮゲートウェイ装置との通信路を暗号化して、ＶＰＮクライアント装置のＩＰアドレス及び共通鍵をＶＰＮゲートウェイ装置に送信する、
ことを特徴とする請求項１乃至３記載のいずれか１項に記載のリモートアクセスＶＰＮ仲介方法。
【請求項５】
ＶＰＮクライアント装置は、ＳＰＫＩ方式に従って証明書を発行し、前記証明書を受信した他のＶＰＮクライアント装置が前記仲介装置に対して、前記ＶＰＮゲートウェイ装置に割り当てられたＩＰアドレスの検索要求を送信することを特徴とする請求項４記載のリモートアクセスＶＰＮ仲介方法。
【請求項６】
ＩＰネットワークにＶＰＮクライアント装置及びＶＰＮゲートウェイ装置が接続され、ＶＰＮゲートウェイ装置により管理されるローカルエリアネットワークに通信装置が接続され、前記ＩＰネットワークに接続された任意のＶＰＮクライアント装置と、ＶＰＮゲートウェイ装置、及び、ＶＰＮゲートウェイ装置に管理されるローカルエリアネットワークに接続された任意の通信装置との間のトンネリングプロトコルによるリモートアクセスＶＰＮを実行するシステムにおいて、

ＩＰネットワーク上に設置されて、リモートアクセスＶＰＮの確立を仲介する仲介装置であって
前記ＶＰＮゲートウェイ装置から送信される前記通信装置に割り当てられたプライベートＩＰアドレスを示す情報（以下、アクセスコントロールリスト）を記憶する手段と、
前記ＶＰＮクライアント装置、前記ゲートウェイ装置を認証し、アクセス権限制御を実行する手段と、
前記アクセスコントロールリストを参照して、前記通信装置に割り当てられたプライベートＩＰアドレスを取得する手段と、
ドメインネームサーバを検索して前記ＶＰＮゲートウェイ装置に割り当てられたＩＰアドレスを取得する手段と、
前記ＶＰＮクライアント装置と前記ＶＰＮゲートウェイ装置との間の認証に用いる共通鍵を生成する手段と、
前記ＶＰＮクライアント装置に、前記ＶＰＮゲートウェイ装置のＩＰアドレス、前記通信装置のプライベートＩＰアドレス及び共通鍵を送信する手段と、
前記ＶＰＮゲートウェイ装置に、前記ＶＰＮクライアント装置のＩＰアドレス及び共通鍵を送信する手段と、
を有することをことを特徴とする仲介装置。
【請求項７】
仲介装置とVPNクライアント装置との間の通信、仲介装置とVPNゲートウェイ装置との間の通信を、それぞれ暗号化する手段を有することを特徴とする請求項６記載の仲介装置。
【請求項８】
前記VPNクライアント装置を認証し、認証に成功した場合に限り、前記VPNゲートウェイ装置に割り当てられたIPアドレスをドメインネームサーバに問い合わせて取得し、共通鍵を生成し、取得したIPアドレスと、前記通信装置に割り当てられたプライベートIPアドレス、及び、生成した共通鍵を前記VPNクライアント装置に送信することを特徴とする請求項6記載の仲介装置。
【請求項９】
前記VPNクライアント装置が前記VPNゲートウェイ装置に割り当てられたIPアドレスを検索する権限を有しているか否かを判定し、権限を有している場合に限り、前記VPNゲートウェイ装置に割り当てられたIPアドレスをドメインネームサーバに問い合わせて取得し、共通鍵を生成し、取得したIPアドレス、前記通信装置に割り当てられたプライベートIPアドレス、及び、生成した共通鍵を前記VPNクライアント装置に送信することを特徴とする請求項6記載の仲介装置。
【請求項１０】
前記VPNゲートウェイ装置を認証し、認証に成功した場合に限り、前記VPNクライアント装置に割り当てられたIPアドレス、及び、前記共通鍵を前記VPNゲートウェイ装置に送信することを特徴とする請求項6記載の仲介装置。
【請求項１１】
SPKI（Simple Public Key Infrasturucture）方式に従って、前記VPNクライアント装置、及び、前記VPNゲートウェイ装置を認証し、及び／または、アクセ権限制御を実行することを特徴とする請求項６乃至１０のいずれか１項に記載の仲介装置。
【請求項１２】
PKI（Public Key Infrasturucture）方式に従って、前記VPNクライアント装置、及び、前記VPNゲートウェイ装置を認証することを特徴とする請求項６乃至１０のいずれか１項に記載の仲介装置。

【書類名】明細書
【発明の名称】リモートアクセスVPN仲介方法及び仲介装置
【技術分野】
【０００１】
本発明は、インターネットにおいて、Ipsec（Ip Security Protocol）、L2TP（Layers2 Tunneling Protocol）等の任意のトンネリングプロトコルによるリモートアクセスVPNを実行するために用いられる情報のうち、VPNクライアント装置のグローバルIPアドレス、VPNゲートウェイ装置のグローバルIPアドレス、VPNクライアント装置とVPNゲートウェイ装置の間で認証に用いる共通鍵等を、VPNクライアント装置とVPNゲートウェイ装置の間で安全に共有する技術に関する。
【背景技術】
【０００２】
インターネット上に構築される仮想の閉域ネットワークは一般にバーチャル プライベート ネットワーク（Virtual Private Network：以後VPNと略す）と呼ばれる。VPNはIPsec、L2TP等のトンネリングプロトコルを用いて構築され、ローカルエリアネットワーク（LAN）内のリソースに移動クライアントからインターネット経由でアクセスしたり、または、物理的に離れた複数のローカルエリアネットワークをインターネット経由で接続する場合に利用される。
【０００３】
トンネリングプロトコルによるリモートアクセスVPNを実現するためには、VPNクライアント装置は、接続先のLANを管理するVPNゲートウェイ装置に割り当てられたグローバルIPアドレスと、接続先であるLAN内の通信装置に割り当てられたプライベートIPアドレスを知る必要がある。また、通信相手を認証し、通信路を暗号化するためには、共通鍵などの鍵情報をVPNクライアント装置とVPNゲートウェイ装置との間で交換することが必要である。
【０００４】
リモートアクセスVPNにおけるローカルエリアネットワーク内の通信装置に対するプライベートIPアドレスの割り当て方法としては、(1) VPNゲートウェイ装置のグローバルIPアドレスと同一のIPアドレスをに割り当てる方法、(2) VPNクライアント装置において、プライベートIPアドレスを静的に割り当てる方法、(3) VPNゲートウェイ装置において、DHCP（Dynamic Host Configration Protocol）、IPCP（PPP IP cotrol Protocol）を用いてアドレスプールから動的に割り当てる方法がある。
【０００５】
上記(1)から(3)に示す方法のうち、(1)及び(2)については、VPNクライアント装置は接続先ホストのプライベートIPアドレスを知る必要がない。しかし、(1)については、ローカルエリアネットワークを構成できないという課題がある。また、(2)については、VPNクライアント装置において任意に接続先のプライベートIPアドレスを指定できるため、VPNゲートウェイ装置においてセキュリティポリシに基づいてローカルエリアネットワークを運用できないという課題がある。また、(3)については、VPNゲートウェイ装置においてプライベートIPアドレスを動的に割り当てるため、VPNクライアント装置は接続先の通信装置に割り当てられたプライベートIPアドレスを知ることができない。
【０００６】
一方、DHCPによってＶＰＮクライアント装置にプライベートIPアドレスを動的に割り当てる方法がある（例えば、非特許文献１参照）。ここでは、VPNクライアント装置は接続先のローカルエリアネットワーク内のプライベートＩＰアドレスを取得してトンネリングプロトコルで接続することにより、ＶＰＮクライアント装置はローカルエリアネットワーク上の仮想的なホストとして動作する。しかしながら、ここに示される方法は、クライアント装置にIPアドレスを割り当てるものであり、クライアント装置が有る接続先のIPアドレスを知るためには別の手段を用いる必要がある。
【０００７】

また、共通鍵を安全に配布する方法としては種々の方法がある（例えば、特許文献１、特許文献２参照）。特許文献１に示される方法は、ローカルエリアネットワークに接続された複数の通信装置との間で共通鍵を交換する方法で、DHCPサーバ機能を有するゲートウェイ装置を介して共通鍵を交換する。具体的には、ローカルエリアネットワークへの接続時にDHCPに従いIPアドレスを取得する際に、共通鍵も同時に交換する。これによって、ローカルエリアネットワーク内の通信を暗号化するための共通鍵を交換できる。また、特許文献２に示される方法は、インターネットに接続されたVPNクライアント装置と、VPNゲートウェイ装置で管理されるローカルエリアに接続された通信装置との通信において、VPNクライアント装置とVPNゲートウェイ装置との間である共通鍵を交換し、VPNゲートウェイ装置と通信装置との間で別の共通鍵を交換する方法である。これによって、VPNクライアント装置とローカルエリアネットワークに接続された通信装置との間でIKE等の鍵交換方式を用いて鍵交換を行う必要なく、VPNクライアント装置とローカルエリアネットワークに接続された通信装置との暗号通信を実現できる。ここに示される方法は、いずれもゲートウェイ装置を介して共通鍵を安全に配布できるが、プライベートIPアドレスを配布する方法については考慮されていない。

【０００８】

また、設定情報を管理する管理装置を設け、管理装置が通信装置に設定情報を転送する際に、通信装置のIPアドレスとログインパスワードを提示してその通信装置にログインし、設定情報を転送する方法がある（例えば、特許文献３参照）。これによれば、ゲートウェイ装置に相当する管理装置から設定情報としてプライベートIPアドレスを配布できるが、IPアドレスとログインパスワードの組み合わせによる認証方法で通信端末の偽装を防ぐことは困難である。それは、IPアドレスは偽装可能であり、パスワードは持ち主を特定できないためである。

【０００９】

また、公開鍵を用いた認証方法、証明書発行方法としてSPKI（Simple Public Key Infrastucture）方式がある（例えば、非特許文献２、非特許文献３）が、リモートアクセスVPNへの利用方法について明らかでない。

【００１０】

【特許文献１】特開2001-292135号

【特許文献２】特開2002-271309号公報

【特許文献３】特開 2003-18163号公報

【非特許文献１】B.Patel,B.Aboba,S.Kelly,V.Gupta,「ダイナミックホスト コンフィグレーション プロトコル （ディーエイチシーピープイ4） コンフィグレーション オブ アイピーセック トンネルモード (Dynamic Host Configration Protocol (DHCPv４） Configration of IPsec Tunnel Mode)」、[online]、2003年1月掲載、RFC3456、Internet Engineering Task Force、[2003年3月17日検索]、インターネット<URL：http://www.ietf.org/rfc/rfc3456.txt>

【非特許文献２】C.Ellison, B.Frantz, B.Lampson, R.Rivest, B.Thomas, T.Ylonen,「エスピーケーアイ サーティフィケート セオリー (SPKI Certificate Theory)」、[online]、1999年9月掲載、RFC2693、Internet Engineering Task Force、インターネット<URL：http://www.ietf.org/rfc/rfc2693.txt>

【非特許文献３】C.Ellison, B.Frantz, B.Lampson, R.Rivest, B.Thomas, T.Ylonen,「シンプル パブリック キー インフラストラクチャ <ドラフトーアイイーティーエフーエスピケーアイーサートーストラクチャー０６．ｔｘｔ> (Simple Public Key Infrastructure <draft-ietf-spki-cert-structure-06.txt>)」, [online]、1999年7月26日掲載、Internet Engineering Task Force、インターネット<URL：http://world.std.com/~cme/spki.txt>

【発明の開示】

【発明が解決しようとする課題】

【００１１】

本発明は、上述のような課題に鑑みなされたものであり、IPネットワークにおいて、IPsec、L2TP等の任意のトンネリングプロトコルによるリモートアクセスVPNを実行するために用いる情報のうち、VPNクライアント装置のグローバルIPアドレス、VPNゲートウェイ装置のグローバルIPアドレス、VPNゲートウェイ装置により管理されるローカルエリアネットワーク内の任意の通信装置のプライベートIPアドレス、及び、VPNクライアント装置とVPNゲートウェイ装置の間でIKEフェーズ1における認証に用いる共通鍵を、VPNクライアント装置とVPNゲートウェイ装置との間で安全に共有できるようにすることである。また、リモートアクセスVPNにおける認証において、利用者の個人情報を通信する相手に知られずに通信できるようにすることである。

【課題を解決するための手段】

【００１２】

本発明は、ＩＰネットワークに、リモートアクセスＶＰＮの動作を仲介する仲介装置を設けたことを主要な特徴とする。

【００１３】

仲介装置は、ＩＰネットワークに接続したVPNクライアント装置、及び、VPNゲートウェイ装置と、VPNゲートウェイ装置により管理されるローカルエリアネットワークに接続した任意の通信装置との間のIPsec、L2TP等の任意のトンネリングプロトコルによるリモートアクセスVPNを確立するために用いる情報（コントロールアクセスリスト）を記憶する。この情報には、通信装置に割り当てられたプライベートIPアドレスが含まれる。

【００１４】

仲介装置は、VPNクライアント装置からVPNゲートウェイ装置に割り当てられたIPアドレスの検索要求を受信したら、VPNクライアント装置がVPNゲートウェイ装置に割り当てられたIPアドレスを検索する権限を有するかどうかを検証する。そして、権限を有する場合に限り、アクセスコントロールリストを参照して、VPNゲートウェイ装置により管理されるローカルエリアネットワークに接続した通信装置に割り当てられたプライベートIPアドレスを取得し、ドメインネームサーバ（DNS）を検索してVPNゲートウェイ装置に割り当てられたIPアドレスを取得し、VPNクライアント装置とVPNゲートウェイ装置との間のIKE等の認証に用いる共通鍵を生成する。次に、仲介装置とVPNクライアント装置との間の通信路を暗号化して、VPNゲートウェイ装置に割り当てられたIPアドレス、通信装置に割り当てられたプライベートIPアドレス及び生成した共通鍵をVPNクライアント装置に送信する。また、仲介装置とVPNゲートウェイ装置との通信路を暗号化して、VPNクライアント装置に割り当てられたIPアドレス及び生成した共通鍵をVPNゲートウェイ装置に送信する。

【００１５】

また、仲介装置は、SPKI方式に従って、VPNクライアント装置、及び、VPNゲートウェイ装置を認証する。また、VPNクライアント装置は、SPKI方式に従って証明書を発行する。さらに、仲介装置はPKI方式に従って、VPNクライアント装置、及び、VPNゲートウェイ装置を認証することも可能とする。

【００１６】

また、仲介装置は、公開鍵、FQDN（Fully Qualified Distinguished Name），GUID（Globally Unique Identifier），MACアドレス，SPKI（Simple Public Key Infrastructure） Local Name，X.500 Distinguish Name等の任意の名前形式に従ってVPNクライアント装置、VPNゲートウェイ装置、及び、通信装置を識別することも可能とする。これによって、IPsec、L2TPなどの任意のトンネリングプロトコル、PKI、SPKI、パスワードなどの任意の認証方式を組み合わせてリモートアクセスVPNを実行できる。

【発明の効果】

【００１７】

本発明においては、次のような効果を奏する。第1の効果は、IPネットワークにおいて、L2TP、IPsec等のトンネリングプロトコルによるリモートアクセスVPNを実行するために用いる情報のうち、VPNクライアント装置のグローバルIPアドレス、VPNゲートウェイ装置のグローバルIPアドレス、VPNゲートウェイ装置により管理されるローカルエリアネット

ワーク内の任意の通信装置のプライベートIPアドレス、及び、VPNクライアント装置とVPNゲートウェイ装置の間でIKEフェーズ1における認証に用いる共通鍵を、VPNクライアント装置とVPNゲートウェイ装置との間で安全に共有できることである。その理由は、仲介装置においてプライベートIPアドレスを安全に管理し、プライベートIPアドレスと共通鍵を安全に配布するためである。

【００１８】

具体的には、プライベートIPアドレスの仲介装置への登録において、VPNゲートウェイ装置を認証し、認証に成功した場合に限り、通信路を暗号化し、暗号化した通信路を用いて、プライベートIPアドレスを受信する。また、プライベートIPアドレスの検索において、VPNクライアント装置を認証し、認証に成功した場合に限り、VPNクライアント装置の公開鍵を用いてアクセス権限制御を実行し、アクセス権限制御に成功した場合に限り、VPNゲートウェイ装置のグローバルIPアドレスをドメインネームサーバDNSに提示して検索し、仲介装置とVPNクライアント装置との間の通信路を暗号化し、暗号化した通信路を用いて、VPNゲートウェイ装置のグローバルIPアドレスと、通信装置のプライベートIPアドレスと、共通鍵をVPNクライアント装置に送信し、また、仲介装置とVPNゲートウェイ装置との通信路を暗号化し、暗号化した通信路を用いて、VPNクライアント装置のグローバルIPアドレスと、共通鍵をVPNゲートウェイ装置に送信するためである。

【００１９】

第２の効果は、リモートアクセスVPNにおける認証において、利用者の個人情報を通信する相手に知られずに通信できる手段を提供することである。その理由は、PKI方式に従って認証する場合には、個人情報を含む公開鍵証明書を通信相手に送信する代わりに仲介装置に送信して認証するためである。また、SPKI方式に従って認証する場合には、いかなる証明書も個人情報を含まないように証明書の形式を定義できるためである。

【発明を実施するための最良の形態】

【００２０】

以下に、本発明の実施の形態について図面を参照して詳細に説明する。

【実施例１】

【００２１】

これは、SPKI（Simple Public Infrastructure）方式に従って、仲介装置がVPNクライアント装置やVPNゲートウェイ装置を認証し、また、VPNクライアント装置が権限委譲の証明書を発行する実施例である。このSPKI方式では認証局は不要である。

【００２２】

図1に本実施例の全体的システム構成を示す。図1において、VPNクライアント装置（A）１０１、VPNクライアント装置（D）１０２、VPNゲートウェイ装置（B）１０３、仲介装置（S）１０４、ドメインネームサーバ（DNS）１０５はそれぞれIP（Internet Protocol）に従ってネットワーク（WAN）１００に接続されている。また。通信装置（C）１１１が、VPNゲートウェイ装置（B）１０３をゲートウェイ装置とするローカルエリアネットワーク（ＬAN）１１０に接続されている。

【００２３】

図２は、図１の全体の動作を説明するための図である。太線はIpsecトンネルモードによるVPNを示している。

【００２４】

ここで、VPNクライアント装置（A）１０１のホスト名は公開鍵PUBLICKEY_A（またはそのハッシュ値HASH_A）、IPアドレスはIPADDRESS_Aとする。VPNクライアント装置（D）１０２のホスト名は公開鍵PUBLICKEY_D（またはそのハッシュ値HASH_D）、IPアドレスはIPADDRESS_Dとする。また、VPNゲートウェイ装置（B）１０３のホスト名は公開鍵PUBLICKEY_B（またはそのハッシュ値HASH_B、IPアドレスはIPADDRESS_B）とする。すなわち、VPNクライアント装置やVPNゲートウェイ装置は、それぞれ、その公開鍵（またはそのハッシュ値）で識別可能である。通信装置（C）１１１のプライベートIPアドレスはIPADDRESS_Cとする。

【００２５】
VPNクライアント装置（A）１０１に割り当てられたIPアドレスIPADDRESS_A、VPNゲートウェイ装置（B）１０３に割り当てられたIPアドレスIPADDRESS_B、及び、VPNクライアント装置（D）１０２に割り当てられたIPアドレスIPADDRESS_Dはいずれもネットワーク（WAN）１００において一意であり、任意の手段で動的に割り当てられる。VPNゲートウェイ装置（B）１０３の公開鍵PUBLICKEY_BとIPアドレスIPADDRESS_Bはドメインネームサーバ（DNS）１０５において一意に関連付けられて管理される。また、通信装置（C）１１１に割り当てられたプライベートIPアドレスIPADDRESS_Cはローカルエリアネットワーク（LAN）１１０において一意であり、任意の手段を用いて動的に割り当てられる。
【００２６】
VPNクライアント装置（A）１０１、VPNクライアント装置（D）１０２、VPNゲートウェイ装置（B）１０３、及び、仲介装置（S）１０４は、IPsecトランスポートモード、または、IPsecトンネルモードにより通信路を暗号化する手段を有する。また、VPNクライアント装置（A）１０１は、公開鍵PUBLICKEY_Aと対の秘密鍵PRIVATEKEY_Aを、PUBLICKEY_Aとともに保管している。VPNゲートウェイ装置（B）１０３は、公開鍵PUBLICKEY_Bと対の秘密鍵PRIVATEKEY_Bを、PUBLICKEY_Bとともに保管している。VPNクライアント装置（D）１０２は、公開鍵PRIVATEKEY_Dとの対の秘密鍵PRIVATEKEY_BをPUBLICKEY_Dとも保管している。VPNゲートウェイ装置（B）１０３は、アクセスコントロールリスト（ACL）を保管している。図６に本実施例におけるアクセスコントロールリスト（ACL）の例を示す。アクセスコントロールリスト（ACL）の文法はSPKI（Simple Public Key Infrastructure）に関する先の非特許文献２、及び非特許文献３で定義されている。
【００２７】
仲介装置（S）１０４は、（１）VPNゲートウェイ装置（B）１０３の公開鍵PUBLICKEY_Bをドメインネームサーバ（CNS）１０５に提示して、VPNゲートウェイ装置（B）１０３に割り当てられたIPアドレスIPADDRESS_Bを取得する手段、（２）VPNゲートウェイ装置（B）１０３で保管されるアクセスコントロールリスト（ACL）を記憶する手段、（３）SPKI方式に基づいて、VPNクライアント装置（A）１０１、VPNゲートウェイ装置（B）１０３を認証し、及び／または、アクセス権限制御を実行する手段、（４）後述の共通鍵KEY_AB、及び、KEY_DBを生成する手段を具備している。
【００２８】
上記（１）の手段では、DNS方式と呼ばれるインターネットにおける一般的な名前解決方式に従って、公開鍵PUBLICKEY_BからIPアドレスIPADDRESS_Bを解決する。また、上記（２）の手段では、公開鍵PUBLICKEY_Bとアクセスコントロールリスト（ACL）を関連付けて管理する。
【００２９】
また、上記（３）の手段では、SPKI方式に従い、VPNクライアント装置（A）、VPNゲートウェイ装置（B）１０３、及び、VPNクライアント装置（D）１０２を認証する。具体的には、秘密鍵PRIVATEKEY_Aによる署名SIG_Aと公開鍵PUBLICKEY_Aをすべて入力して、署名SIG_Aを確認することにより、秘密鍵PRIVATEKEY_Aの本人性を証明する。同様に、秘密鍵PRIVATEKEY_Bによる署名SIG_Bと公開鍵PUBLICKEY_Bをすべて入力して、署名SIG_Bを確認することにより、秘密鍵PRIVATEKEY_Bの本人性を証明する。同様に、秘密鍵PRIVATEKEY_Dによる署名SIG_D、及び、公開鍵PUBLICKEY_Dをすべて入力して、署名SIG_Dを確認することにより、秘密鍵PRIVATEKEY_Dの本人性を証明する。また、上記（３）の手段では、SPKI方式に従い、VPNゲートウェイ装置（B）１０３に対するVPNクライアント装置（A）１０１、及び、VPNクライアント装置（D）１０２のアクセス権限を制御する。VPNゲートウェイ装置（B）１０３に対するVPNクライアント装置（A）１０１のアクセス権限を制御する場合には、VPNゲートウェイ装置（B）１０３のIPアドレスIPADDRESS_Bを検索するためのDNSクエリQUERY、署名SIG_A、及び、アクセスコントロールリスト（ACL）を入力して、SPKIに関する非特許文献2、及び、非特許文献3において定義される5-tuple reduction演算規則、及び／または、4-tuple reduction演算規則に基づく演算を実行して、演算結果を出力

する。また、VPNゲートウェイ装置（B）１０３に対するVPNクライアント装置（D）１０２のアクセス権限を制御する場合には、VPNゲートウェイ装置（B）１０３のIPアドレスIPADDRESS_Bを検索するためのDNSクエリQUERY、署名SIG_D、SPKIに関する非特許文献2及び非特許文献3において定義される証明書CERT、及び、アクセスコントロールリスト（ACL）を入力して、SPKIに関する非特許文献2、及び、非特許文献3において定義される5-tuple reduction演算規則、及び／または、4-tuple reduction演算規則に基づく演算を実行して、演算結果を出力する。演算結果の具体例については、図８を参照して後述する。

【００３０】

また、上記（４）の手段は、VPNクライアント装置（A）１０１とVPNゲートウェイ装置（B）１０３との間のIKEフェーズ1における認証に用いる共通鍵KEY_AB、または、VPNクライアント装置（D）１０２とVPNゲートウェイ装置（B）１０３との間のIKEフェーズ1における認証に用いるKEY_DBをそれぞれ生成する。

【００３１】

また、VPNクライアント装置（A）１０１は、SPKI方式に従って、VPNクライアント装置（D）１０２に対し言言委譲の証明書CERTを発行する機能を有する。SPKIに関する非特許文献2及び非特許文献3においては、権限証明書（Authorization Certificate）と名前証明書（Name Certificate）の２種類の証明書について、それぞれ文法を定義している。本実施例においては、説明を簡単にするために、証明書CERTは権限証明書の１種類であると定義する。図９に本実施例における証明書CERTの具体例を示す。SPKIに関する非特許文献２及び非特許文献３によれば、権限証明書は、発行者の秘密鍵と一意に対応した公開鍵またはその公開鍵のハッシュ値を定義するissuerフィールド、権限の行使者の秘密鍵と一意に対応した公開鍵またはその公開鍵のハッシュ値を定義するsubjectフィールド、権限内容を定義した文字列を含むtagフィールド、権限委譲を許可するか否かを定義した文字列を含むdelegationフィールド、及び、権限証明書の有効期間を定義した文字列を含むvalidityフィールドから構成されるデータ（以後、本データを証明書情報INFOと呼ぶ）に対し、発行者の秘密鍵で署名したデータである。この定義に基づき、本実施例における証明書CERTの証明書情報INFOにおけるissuerフィールドの値は、公開鍵PUBLICKEY_Aまたは任意のハッシュ演算アルゴリズムによる公開鍵PUBLICKEY_Aのハッシュ値HASH_Aであると定義する。かつ、subjectフィールドの値は、公開鍵PUBLICKEY_Dまたは任意のハッシュ演算アルゴリズムによる公開鍵PUBLICKEY_Dのハッシュ値HASH_Dであると定義する。かつ、tagフィールドの値は、VPNゲートウェイ装置（B）１０３のIPアドレスIPADDRESS_Bであると定義する。かつ、delegationフィールドの値は、非特許文献２において定義される文字列「(propagate)」であると定義する。一方、validityフィールドの値は、本発明とは直接関係しないため、いかなる値も定義しないものとする。また、証明書情報INFOに秘密鍵PRIVATEKEY_Aを用いて署名する。

【００３２】

次に、図２を参照して、図１の動作概要を説明する。アクセスコントロール（ACL）の登録（記憶）時、VPNゲートウェイ装置（Ｂ）１０３は、公開鍵PUBLICKEY_B（またはそのHASH_B）とアクセスコントロール（ACL）を仲介装置（S）１０４に送信する（ステップ１）。仲介装置（S）１０４は該公開鍵PUBLICKEY_B（またはそのHASH_B）とアクセスコントロール（ACL）を記憶する。

【００３３】

VPNゲートウェイ装置（B）１０３を経由して、VPNクライアント装置（A）１０１から通信装置（C）１１１にIpsecトンネルモードによるリモートVPNを実行する場合、VPNクライアント装置（A）１０１は、公開鍵PUBLICKEY_Aと公開鍵PUBLICKEY_B（またはそのHASH_B）（を仲介装置（S）１０４に送信して、VPNゲートウェイ装置（Ｂ）１０３及び通信装置（C）IPアドレスの検索要求を行なう（ステップ２）。

【００３４】

仲介装置（S）１０４は、SPKI方式に従ってVPNクライアント装置（A）１０１のアクセス権限制御を実行し、アクセスを許可する場合には、ドメインネームサーバ（DNS）１０

５を検索してVPNゲートウェイ装置（Ｂ）１０３に割り当てられたIPアドレスIPADDRESS_Bを取得する（ステップ３）。また、仲介（S）１０４は、アクセスコントロール（ACL）を参照して、VPNゲートウェイ装置（Ｂ）１０３により管理されるLAN１１０に接続された通信装置（C）１１１に割り当てられたプライベートIPアドレスIPADDRESS_Cを取得する。さらに、仲介装置（S）１０４は、VPNクライアント装置（A）１０１との間の認証に用いる共通鍵KEY_ABを生成する。そして、仲介装置（S）１０４は、仲介装置（S）１０４とVPNクライアント装置（A）１０１との間の通信路を暗号化し、VPNクライアント装置（A）１０１へIPADDRESS_B、IPADDRESS_C及び共通鍵KEY_ABを送信する（ステップ４）。また、仲介装置（S）１０４は、仲介装置（S）１０４とVPNゲートウェイ装置（Ｂ）１０３との間の通信路を暗号化し、VPNゲートウェイ装置（Ｂ）１０３へIPADDRESS_AとKEY_ABを送信する（ステップ５）。

【００３５】

また、VPNクライアント装置（A）１０１は、VPNゲートウェイ装置（B）１０３のIPアドレスを検索する権限をVPNクライアント装置（D）１０２委譲する場合、VPNクライアント装置（D）１０２に対してSPKI方式に従って証明書CERTを送信する（ステップ６）。VPNクライアント装置（D）１０２は、公開鍵PUBLICKEY_DとCERT、及び公開鍵PUBLICKEY_B（またはそのHASH_B）仲介装置（S）１０４に送信して、VPNゲートウェイ装置（B）１０３及び通信装置（C）のIPアドレスの検索要求を行なう（ステップ７）。

【００３６】

仲介装置（S）１０４は、SPKI方式に従ってVPNクライアント装置（D）１０２のアクセス権限制御を実行し、アクセスを許可する場合には、ドメインネームサーバ（DNS）１０５を検索してVPNゲートウェイ装置（Ｂ）１０３に割り当てられたIPアドレスIPADDRESS_Bを取得する（ステップ８）。また、仲介装置（S）１０４は、アクセスコントロール（ACL）を参照して、VPNゲートウェイ装置（Ｂ）１０３により管理されるLAN１１０に接続された通信装置（C）１１１に割り当てられたプライベートIPアドレスIPADDRESS_Cを取得する。さらに、仲介装置（S）１０４は、VPNクライアント装置（D）１０２との間の認証に用いる共通鍵KEY_DBを生成する。そして、仲介装置（S）１０４は、仲介装置（S）１０４とVPNクライアント装置（D）１０２との間の通信路を暗号化し、VPNクライアント装置（d）１０２へIPADDRESS_B、IPADDRESS_C及び共通鍵KEY_DBを送信する（ステップ９）。また、仲介装置（S）１０４は、仲介装置（S）１０４とVPNゲートウェイ装置（Ｂ）１０３との間の通信路を暗号化し、VPNゲートウェイ装置（Ｂ）１０３へIPADDRESS_DとKEY_DBを送信する（ステップ１０）。

【００３７】

以上、図１に示すシステムの各装置の構成及び全体の動作概要を述べたが、ドメインネームサーバ（DNS）１０５におけるIPアドレスの管理及び名前解決方法、IPsecトランスポートモードまたはトンネルモードによる通信路の暗号化方法、共通鍵KEY_AB及びKEY_DBの生成方法、及び、公開鍵を用いた署名確認方法については、当業者にとってよく知られているので、その詳細な構成は省略する。また、SPKI方式におけるアクセス権限制御において、権限証明書に加え、名前証明書を用いる場合も本実施例と同様の方法で実施できるため、その詳細な説明については省略する。

【００３８】

以下に、本実施例１におけるアクセスコントロールリスト（ACC）の記憶手順、及びIPアドレスの取得共通鍵の生成、これらIPアドレスと共通鍵の送信手順について詳述する。

【００３９】

まず、図３を参照して、VPNゲートウェイ装置（B）１０３において保管されるアクセスコントロールリスト（ACL）を仲介装置（S）１０４に記憶する手順について説明する。

VPNゲートウェイ装置（B）１０３と仲介装置（S）１０４は、IPsecトランスポートモードにより接続する（ステップ１００１）。これでVPNゲートウェイ装置（B）１０３と仲介装置（S）１０４との間の通信路が暗号化される。VPNゲートウェイ装置（B）１０３は、暗号化された通信路を用いて、公開鍵PUBLICKEY_BとSKPI形式のアクセスコントロールリ

スト（ACL）（図６）をすべて送信する（ステップ１００２）。仲介装置（S）１０４は、VPNゲートトウェイ装置（B）１０３から送信された公開鍵PUBLICKEY_Bとアクセスコントロールリスト（ACL）を受信して、該受信した公開鍵PUBLICKEY_Bとアクセスコントロールリスト（ACL）を関連づけて記憶する（ステップ１００３）。VPNゲートウェイ装置（B）１０３と仲介装置（S）１０４は、接続を切断する（ステップ１００４）。

次に、図４及び図５を参照して、仲介装置（S）１０４が、VPNクライアント装置（A）１０１とVPNゲートウェイ装置（B）１０３との間の共通鍵KEY_ABを生成し、VPNゲートウェイ装置（B）１０３に割り当てられたIPアドレスIPADDRESS_B、通信装置（C）に割り当てられたプライベートIPアドレスIPADDRESS_C、及び、共通鍵KEY_ABをVPNクライアント装置（A）１０１に送信し、また、VPNクライアント装置（A）１０１に割り当てられたIPアドレスIPADDRESS_A、及び、共通鍵KEY_ABをVPNゲートウェイ装置（B）１０３に送信する手順について説明する。

【００４０】

図４において、ＶＰＮクラアント装置（Ａ）１０１と仲介装置（Ｓ）１０４は、ＩＰsecトランスポートモードにより接続する（ステップ１１０１）。すなわち、ＶＰＮクライアント装置（A）１０１と仲介装置（S）１０４との間の通信路が暗号化される。VPNクライアント装置（A）１０１は、暗号化された通信路を用いて、VPNゲートウェイ装置（B）１０３の公開鍵PUBLICKEY_Bを含むDNSクエリQUERY、及び、VPNクライアント装置（A）１０１の公開鍵PUBLICKEY_Aをすべて送信する（ステップ１１０２）。

【００４１】

仲介装置（S）１０４は、VPNクライアント装置（A）１０１に割り当てられたIPアドレスIPADDRESS_A、VPNゲートウェイ装置（B）１０３に割り当てられたIPアドレスにIPアドレスIPADDRESS_B、VPNゲートウェイ装置（B）１０３により管理されるLAN１１０に接続される通信装置（C）１１１に割り当てられたプライベートIPアドレスIPADDRESS_Cを取得し、VPNクライアント装置（A）１０１とVPNゲートウェイ装置（B）１０３との間のIKE等の認証に用いる共通鍵KEY_ABを生成する（ステップ１１０３）。図５はステップ１１０３の詳細処理フローである。

【００４２】

図５において、仲介装置（Ｓ）１０４は、ＶＰＮクライアント装置（Ａ）１０１から送信されたDNSクエリQUERYと公開鍵PUBLICKEY_Aをすべて受信して入力する（ステップ１２０１）。次に、入力したDNSクエリQUERYを参照して、公開鍵PUBLICKEY_Bをすべて取得する（ステップ１２０２）。次に、取得した公開鍵PUBLICKEY_Bをもとに、関連付けられたアクセスコントロールリスト（ACL）をすべて取得する（ステップ１２０３）。アクセスコントロールリスト（ACL）は図６に示す形式をとる。次に、ステップ１２０１において入力したDNSクエリQUERYを用いて、図７に示す形式のデータTAGを生成する（ステップ１２０４）。

【００４３】

仲介装置（S）１０４は、上記ステップ１２０１において入力した公開鍵PUBLICKEY_Aとステップ１２０４において生成したデータTAGとステップ１２０３において取得したアクセスコントロールリスト（ACL）をすべて入力し、例えば、非特許文献2、及び、非特許文献3 において定義される演算規則に従って演算を実行し（ステップ１２０５）、演算に成功する否か判定する（ステップ１２０６）。演算に失敗した場合、この時点で処理を終了とする。

【００４４】

仲介装置（S）１０４は、ステップ１２０６において、演算に成功した場合と判定された場合に限り、図８に示す形式の演算結果のデータDATAを出力する。図８に示す演算結果データDATAは非特許文献2、及び、非特許文献3で定義される5-tuple形式のデータである。演算結果データDATAのsubjectフィールドの値がステップ１２０１において受信した公開鍵PUBLICKEY_AのSHA-1アルゴリズムによるハッシュ値HASH_Aと完全一致しているACLエントリが、ステップ１２０３において取得したアクセスコントロールリスト（ACL）に含

まれる場合に限り、データDATAのtagフィールドにはデータTAGと完全一致する文字列が含まれる。

【００４５】

仲介装置（S）１０４は、出力されたデータDATAのtagフィールドを参照して、DNSクエリQUERY'を生成する（ステップ１２０７）。次に、DNSクエリQUERY'をドメインネームサーバ（DNS）１０５に提示して検索し、IPアドレスIPADDRESS_Bを取得する（ステップ１２.０８）。次に、公開鍵PUBLICKEY_Aのハッシュ値HASH_AをもとにアクセスコントロールリストACLを検索し、(subjectフィールドの値にハッシュ値HASH_Aと完全一致する文字列を含む（ACL）エントリENTRYを取得する（ステップ１２０９）。次に、ステップ１２０９において取得したACLエントリENTRYのtagフィールドを参照して、プライベートIPアドレスIPADDRESS_Cを取得する（ステップ１２１０）。次に、VPNクライアント装置（A）１０１のIPアドレスIPADDRESS_Aを取得する（ステップ１２１１）。次に、共通鍵KEY_ABを生成する（ステップ１２１２）。

【００４６】

図４に戻り、仲介装置（S）１０４は、ステップ１１０１において暗号化された通信路を用いて、上記取得したIPアドレスIPADDRESS_B、取得したプライベートIPアドレスIPADDRESS_C、及び、生成した共通鍵KEY_ABをすべてVPNクライアント装置（A）１０１に送信する（ステップ１１０４）。次に、クライアント装置（A）１０１と仲介装置（S）１０４は、接続を切断する（ステップ１１０５）。

【００４７】

次に、VPNゲートウェイ装置（B）１０３と仲介装置（S）１０４は、IPsecトランスポートモードにより接続する（ステップ１１０６）。すなわち、VPNゲートウエイ装置（B）１０３と仲介装置（S）１０４との間の通信路が暗号化される。次に、仲介装置（S）１０４は、ステップ１１０６において暗号化された通信路を用いて、先に取得したIPアドレスIPADDRESS_A、及び、先にて生成した共通鍵KEY_ABをすべてVPNゲートウェイ装置（B）１０３に送信する（ステップ１１０７）。次に、VPNゲートウェイ装置（B）１０３と仲介装置（S）１０４は、接続を切断する（ステップ１１０８）。

【００４８】

その後、図２に示したようなVPNゲートウェイ装置（B）１０３を経由して、クライアント装置（A）１０１から通信装置（C）１１１にIpsecトンネルモードによるリモートアクセスVPNが実行されるが、その詳細は省略する。

【００４９】

次に、VPNクライアント装置（A）１０１において証明書CERTを発行し、発行した証明書CERTをVPNクライアント装置（D）１０２に渡す手順を以下に示す。なお、その処理フロー図は省略する。

(1) VPNクライアント装置（A）１０１は、SPKI方式において定義された文法に従い、証明書CERTの証明書情報INFOを生成する。本実施例における証明書CERTの実施例を図９に示す。図９において、証明書情報INFOにおけるissuerフィールドの値は、公開鍵PUBLICKEY_Aの任意のハッシュ演算アルゴリズムによるハッシュ値HASH_Aであると定義する。かつ、subjectフィールドの値は、公開鍵PUBLICKEY_DのSHA-1アルゴリズムによるハッシュ値HASH_Dであると定義する。かつ、tagフィールドの値は、VPNゲートウェイ装置Bに割り当てられたIPアドレスIPADDRESS_Bであると定義する。かつ、delegationフィールドの値は、非特許文献3において定義される文字列「(propagate)」であると定義する。一方、validityフィールドの値は、本発明とは直接関係しないため、任意の値を定義してもよい。

(2) VPNクライアント装置（A）１０１は、上記（1）において生成したデータに秘密鍵PRIVATEKEY_Aを用いて署名することにより、証明書CERTを発行する。

(3) VPNクライアント装置（A）１０１は、上記（2）において発行した証明書CERTを任意の手段でVPNクライアント装置（D）１０２にすべて送信する。

(4) VPNクライアント装置（D）１０２は、VPNクライアント装置（A）１０から送信された証明書CERTを任意の手段ですべて受信し、記憶する。

【００５０】
仲介装置（S）１０４が、VPNクライアント装置（D）１０２とVPNゲートウェイ装置（B）１０３との間のIKE等の認証に用いる共通鍵KEY_DBを生成し、次に、IPアドレスIPADDRESS_B、プライベートIPアドレスIPADDRESS_C、及び、共通鍵KEY_DBをVPNクライアント装置（D）１０２に送信し、次に、VPNクライアント装置（D）１０２に割り当てられたIPアドレスIPADDRESS_D、及び、共通鍵KEY_DBをVPNゲートウェイ装置（B）１０３に送信する手順は、先の図４及び図５において説明した仲介装置（S）が、VPNクライアント装置（A）１０１とVPNゲートウェイ装置（B）１０３との間の共通鍵KEY_ABを生成して、IPアドレスIPADDRESS_B、プライベートIPアドレスIPADDRESS_C、及び、共通鍵KEY_ABをVPNクライアント装置（A）１０１に送信し、また、IPアドレスIPADDRESS_A、及び、共通鍵KEY_ABをVPNゲートウェイ装置（B）１０３に送信する手順と同様の手順で実施できる。
【００５１】
このようにして、図２に示したように、VPNゲートウェイ装置（B）１０３を経由して、VPNクライアント装置（D）１０２からも通信装置（C）１１１にIpsecトンネルモードによるリモートアクセスVPNが実行することが可能になる。
【００５２】
以上述べたように、本実施例において、仲介装置（S）１０４は、VPNゲートウェイ装置（B）１０３より送信されたアクセスコントロールリスト（ACL）を記憶することで、通信装置（C）１１１に割り当てられたプライベートIPアドレスIPADDRESS_Cを記憶する。これによって、仲介装置（S）１０４は、VPNゲートウェイ装置（B）１０３だけが知っている、ローカルエリアネットワーク（LAN）１１０に接続された通信装置（C）１１１に割り当てられたプライベートIPアドレスIPADDRESS_Cを知ることができる。従って、VPNクライアント装置（A）１０１は、VPNゲートウェイ装置（B）１０３を介した通信装置（C）１１１へのIPsecトンネルモードによるリモートアクセスVPNに必要なプライベートIPアドレスIPADDRESS_Cを、リモートアクセスVPNを実行する前に仲介装置（S）１０４に問い合わせることにより知ることができる。
【００５３】
また、本実施例において、仲介装置（S）１０４は、共通鍵KEY_ABを生成し、生成した共通鍵KEY_ABをVPNクライアント装置（A）１０１とVPNゲートウェイ装置（B）１０３の両者に送信する。これによって、VPNクライアント装置（A）１０１とVPNゲートウェイ装置（B）１０３はともに共通鍵KEY_ABを受信できる。従って、VPNクライアント装置（A）１０１とVPNゲートウェイ装置（B）１０３はIKEフェーズ1における認証に用いる共通鍵KEY_ABをオンラインで共有できる。
【００５４】
また、本実施例において、仲介装置（S）１０４は、VPNゲートウェイ装置（B）１０３を認証し、認証に成功した場合に限り、VPNゲートウェイ装置（B）１０３より送信された、通信装置（C）１１１に割り当てられたプライベートIPアドレスIPADDRESS_Cを、仲介装置（S）１０４に記憶する。これによって、仲介装置（S）１０４は、偽装されていないVPNゲートウェイ装置（B）１０３から送信されたプライベートIPアドレスIPADDRESS_Cに限り記憶できる。従って、VPNクライアント装置（A）１０１は、正しいVPNゲートウェイ装置（B）１０３から送信されたプライベートIPアドレスIPADDRESS_Cを知ることができる。
【００５５】
また、本実施例において、仲介装置（S）１０４は、VPNゲートウェイ装置（B）１０３を認証し、認証に成功した場合に限り、VPNゲートウェイ装置（B）１０３より送信された、通信装置（C）１１１に割り当てられたプライベートIPアドレスIPADDRESS_Cを記憶するという動作において、仲介装置（S）１０４とVPNゲートウェイ装置（B）１０３との間の通信路を暗号化する。これによって、仲介装置（S）１０４は、VPNゲートウェイ装置（B）１０３から送信された、通信装置（C）１１１に割り当てられたプライベートIPアドレスIPADDRESS_Cを改ざんされることなく、かつ、盗聴されることなく受信できる。従って、VPNクライアント装置（A）１０１は、正しいVPNゲートウェイ装置（B）１０３から送信

された、通信装置（C）１１１に割り当てられた正しいプライベートIPアドレスIPADDRESS_Cを知ることができる。また、VPNゲートウェイ装置（B）１０３、通信装置（C）１１１に割り当てられた正しいプライベートIPアドレスIPADDRESS_Cを不特定多数に知られることなく仲介装置（S）１０４に送信できる。

【００５６】

また、本実施例において、仲介装置（S）１０４は、VPNクライアント装置（A）１０１を認証し、認証に成功した場合に限り、VPNゲートウェイ装置（B）１０３に割り当てられたIPアドレスIPADDRESS_Bをドメインネームサーバ（DNS）１０５に問い合わせて取得し、共通鍵KEY_ABを生成し、取得したIPアドレスIPADDRESS_B、通信装置Cに割り当てられたIPアドレスIPADDRESS_B、及び、生成した共通鍵KEY_ABをすべてVPNクライアント装置（A）１０１に送信するという動作を実行する。これによって、仲介装置（S）１０４は、VPNクライアント装置（A）１０１が偽装されていない場合に限り、VPNゲートウェイ装置（B）１０３に割り当てられたIPアドレスIPADDRESS_B、通信装置（C）１１１に割り当てられたプライベートIPアドレスIPADDRESS_C、及び、共通鍵KEY_ABのすべてをVPNクライアント装置（A）１０１に送信できる。従って、正しいVPNクライアント装置（A）１０１に限り、VPNゲートウェイ装置（B）１０３を介して、通信装置（C）１１１とIPsecトンネルモードによるリモートアクセスVPNを実行できる。

【００５７】

また、本実施例において、仲介装置（S）１０４は、VPNクライアント装置（A）１０１がVPNゲートウェイ装置（B）１０３に割り当てられたIPアドレスIPADDRESS_Bを検索する権限を有しているか否かを判定し、権限を有している場合に限り、VPNゲートウェイ装置（B）１０３に割り当てられたIPアドレスIPADDRESS_Bをドメインネームサーバ（DNS）１０５に問い合わせて取得し、共通鍵KEY_ABを生成し、取得したIPアドレスIPADDRESS_B、通信装置（C）１１１に割り当てられたIPアドレスIPADDRESS_B、及び、生成した共通鍵KEY_ABをすべてVPNクライアント装置（A）１０１に送信するという動作を実行する。これによって、仲介装置（S）１０４は、VPNゲートウェイ装置（B）１０３に割り当てられたIPアドレスIPADDRESS_B、通信装置（C）１１１に割り当てられたプライベートIPアドレスIPADDRESS_C、及び、共通鍵KEY_ABのすべてを、VPNゲートウェイ装置（B）１０３、及び、通信装置（C）１１１に対しあらかじめアクセス権限を有するVPNクライアント装置（A）１０１だけに送信できる。従って、VPNゲートウェイ装置（B）１０３、及び、通信装置（C）１１１に対する、不特定多数からのIPsecトンネルモードによるリモートアクセスVPNを防止できる。

【００５８】

また、本実施例において、仲介装置（S）１０４は、仲介装置（S）１０４とVPNクライアント装置（A）１０１との間の通信を暗号化する。これによって、仲介装置（S）１０４は、VPNゲートウェイ装置（B）１０３に割り当てられたIPアドレスIPADDRESS_B、通信装置（C）１１１に割り当てられたプライベートIPアドレスIPADDRESS_C、及び、共通鍵KEY_ABを改ざんされることなく、かつ、盗聴されることなくVPNクライアント装置（A）１０１に送信できる。従って、VPNクライアント装置（A）１０１は、正しいVPNゲートウェイ装置（B）１０３を介して、正しい通信装置（C）１１１と、IPsecトンネルモードによるリモートアクセスVPNを実行できる。

【００５９】

また、本実施例において、仲介装置（S）１０４は、VPNゲートウェイ装置（B）１０３を認証し、認証に成功した場合に限り、VPNクライアント装置（A）１０１に割り当てられたIPアドレスIPADDRESS_A、及び、共通鍵KEY_ABをVPNゲートウェイ装置（B）１０３に送信するという動作を実行する。これによって、仲介装置（S）１０４は、VPNゲートウェイ装置（B）１０３が偽装されていない場合に限り、VPNクライアント装置（A）１０１に割り当てられたIPアドレスIPADDRESS_A、及び、共通鍵KEY_ABをVPNゲートウェイ装置（B）１０３に送信できる。従って、VPNクライアント装置（A）１０１は、正しいVPNゲートウェイ装置（B）１０３を介して、通信装置（C）１０４とIPsecトンネルモードによるリモ

ートアクセスVPNを実行できるという効果が得られる。

【００６０】

また、本実施例において、仲介装置（S）１０４は、VPNゲートウェイ装置（B）１０３を認証し、認証に成功した場合に限り、VPNクライアント装置（A）１０１に割り当てられたIPアドレスIPADDRESS_A、及び、共通鍵KEY_ABをVPNゲートウェイ装置（B）１０３に送信するという動作において、仲介装置（S）１０４とVPNゲートウェイ装置（B）１０３との間の通信を暗号化するという動作を実行する。これによって、仲介装置（S）１０４は、VPNクライアント装置（A）１０１に割り当てられたIPアドレスIPADDRESS_A、及び、共通鍵KEY_ABをすべて改ざんされることなく、かつ、盗聴されることなくVPNゲートウェイ装置Bに送信できる。従って、VPNゲートウェイ装置（B）１０３、及び、通信装置（C）１１１は、正しいVPNクライアント装置（A）１０１と、IPsecトンネルモードによるリモートアクセスVPNを実行できる。

【００６１】

また、本実施例において、仲介装置（S）１０４は、SPKI方式に従って、VPNクライアント装置（A）１０１、及び、VPNゲートウェイ装置（B）１０３を認証すると。これによって、署名確認による本人性証明が可能なため、VPNクライアント装置（A）１０１、及び、VPNゲートウェイ装置（B）１０３の両者とも仲介装置（S）１０４に公開鍵証明書を送信する必要がなくなる。従って、VPNクライアント装置（A）１０１の個人情報もVPNゲートウェイ装置（B）１０３の個人情報の両者を仲介装置Sに対して隠蔽できる。

【００６２】

また、本実施例において、VPNクライアント装置（A）１０１は、SPKI方式に従って証明書CERTを発行し、VPNクライアント装置（D）１０２に送信する。これによって、VPNクライアント装置（A）１０１は、VPNクライアント装置（D）１０２に対して、VPNゲートウェイ装置（B）１０３に割り当てられたIPアドレスIPADDRESS_Bを検索する権限を委譲できるため、VPNクライアント装置（D）１０２、VPNゲートウェイ装置（B）１０３に割り当てられたIPアドレスIPADDRESS_Bを検索することができる。かつ、通信装置（C）１１１に割り当てられたプライベートIPアドレスIPADDRESS_Cを知ることができる。従って、VPNクライアント装置（D）１０２も、VPNゲートウェイ装置（B）１０３を介して通信装置（C）１１１とIPsecトンネルモードによるリモートアクセスVPNを実行できるという効果が得られる。また、これによって、VPNゲートウェイ装置（B）１０３は他のVPNクライアント装置（D）１０２についての情報をアクセスコントロールリスト（ACL）に追加する必要なく、他のVPNクライアント装置（D）１０２からのリモートアクセスVPNを許可することができる。従って、VPNゲートウェイ装置（B）１０３は、アクセスコントロールリスト（ACL）の編集などの管理作業に要するコストを軽減できる。

【００６３】

なお、図１、図２に示すドメインネームサーバ（DNS）１０５において、公開鍵PUBLICKEY_Bのハッシュ値HASH_BとIPADDRESS_Bを関連付けて管理する場合、VPNゲートウェイ装置（B）１０３は公開鍵PUBLICKEY_Bのハッシュ値HASH_Bを生成してから、ハッシュ値HASH_BとIPアドレスIPADDRESS_Bをドメインネームサーバ DNSに登録し、かつ、図４に示す手順（ステップ１１０２）を、公開鍵PUBLICKEY_Bの任意のハッシュ演算アルゴリズムによるハッシュ値HASH_Bを含むDNSクエリQUERYに変更することにより明らかに実施できる。

【００６４】

また、図６に示すアクセスコントロールリスト（ACL）、図７に示すデータTAG、図８に示す演算結果のデータDATA、及び、図９に示す証明書CERTにおいて、SHA-1アルゴリズムの他の任意のハッシュ演算アルゴリズムを用いてハッシュ値HASH_Aを演算してもよい。また、issuerフィールドの値をハッシュ値HASH_Aの代わりに公開鍵PUBLICKEY_Aであると定義してもよい。同様に、subjectフィールドの値をハッシュ値HASH_Dの代わりに公開鍵PUBLICKEY_Dと定義してもよい。本変更を実施しても、SPKIに関する非特許文献2及び非特許文献3において定義される演算規則に従って演算することにより、アクセス制御に関して等しい実行結果が得られる。SHA-1アルゴリズム以外のハッシュ演算アルゴリズムを用い

る場合の証明書CERTの形式、及び、issuerフィールド及びsubjectフィールドに公開鍵を指定する場合のアクセスコントロールリストACL、データDATA、及び、証明書CERTの形式については、SPKIに関する非特許文献3において詳細に説明されているため、その詳細な説明については省略する。本変更に伴い、図５に示す手順（ステップ１２０９）を公開鍵PUBLICKEY_Aを提示してアクセスコントロールリストACLを検索し、ACLエントリENTRYを取得する手順に変更することにより明らかに実施できる。

【００６５】

また、図２に示すVPNクライアント装置（A）１０１にはグローバルIPアドレスIPADDRESS_Aのみを割り当てているが、これに加えて、仲介装置（S）１０４において、非特許文献1に示す方法等を用いてローカルエリアネットワークLAN内の任意のプライベートIPアドレスも割り当てても良い。

【実施例２】

【００６６】

本実施例は、証明書CERTについてさらに工夫し、証明書CERTをX.509形式の公開鍵証明書としたものである。基本的なシステム構成は先の実施例１と同様であるが、認証局が必要である。　図１０に本実施例の全体的システム構成を示す。図１０において、VPNクライアント装置（A）１０１、VPNゲートウェイ装置（B）１０３、認証局（CA）１０６、ドメインネームサーバ（DNS）１０５、及び、仲介装置（S）１０４はいずれもIP（Internet Protocol）に従ってネットワーク（WAN）１００に接続されている。また、通信装置（C）１１１はVPNゲートウェイ装置（B）１０３をゲートウェイ装置とするローカルエリアネットワーク（LAN）１１０に接続されてる。

【００６７】

図１１は、図１０の全体の動作を説明するための図である。太線はIPsecトンネルモードによるリモートアクセスVPN、点線はIKEフェーズ１における認証において、認証局（CA）１０６に公開鍵証明書CERTを提示することを示している。ここでも、VPNクライアント装置（A）１０１のホスト名は公開鍵PUBLICKEY_A（またはそのハッシュ値HASH-A）、ＩＰアドレスはIPADDRESS_A、VPNゲードウェイ装置(B）１０３のホスト名は公開鍵PUBLICKEY_B（またはハッシュ値HASH-B)、IPアドレスはIPADDRESS_B、または、通信装置（C）１１１のプライベートIPアドレスはIPAＥSS_Cとする。

【００６８】

VPNクライアント装置（A）１０１に割り当てられたIPアドレスIPADDRESS_A、及び、VPNゲートウェイ装置（B）１０３に割り当てられたIPアドレスIPADDRESS_BはいずれもＩＰネットワーク（WAN）１００内で一意であり、任意の手段で動的に割り当てられる。VPNゲートウェイ装置（B）１０３の公開鍵PUBLICKEY_B（またはＨＡＳＨ－Ｂ）とIPアドレスIPADDRESS_Bはドメインネームサーバ（DNS）１０５において一意に関連付けて管理される。通信装置（C）１１１に割り当てられたプライベートIPアドレスIPADDRESS_Cはローカルエリアネットワーク（LAN）１１０においてのみ一意であり、DHCP（Dynamic Host Configuration Protocol）、IPCP（PPP IP control protocol）等の任意の手段を用いて動的に割り当てられる。

【００６９】

VPNクライアント装置（A）１０１、VPNゲートウェイ装置（B）１０３、及び、仲介装置（S）１０４は、いずれも、IPsecトランスポートモード、または、IPsecトンネルモードにより通信路を暗号化する手段を有する。公開鍵PUBLICKEY_Aの秘密鍵はPRIVATEKEY_Aで、VPNクライアント装置（A）１０１で保管される。CERT_Aは、秘密鍵PRIVATEKEY_Aと対となる公開鍵PUBLICKEY_Aを含むX.509形式の公開鍵証明書で、認証局（CA）１０６の秘密鍵PRIVATEKEY_Sで署名され、VPNクライアント装置（A）１０１で保管される。また、公開鍵PUBLICKEY_Ｂの秘密鍵PRIVATEKEY_Bは、VPNゲートウェイ装置（B）１０３で保管される。CERT_Bは、秘密鍵PRIVATEKEY_Bと対となる公開鍵PUBLICKEY_Bを含むX.509形式の公開鍵証明書で、同じく認証局（CA）１０６の秘密鍵PRIVATEKEY_Sで署名され、VPNゲートウェイ装置(B)１０３で保管される。認証局（CA）１０６は、PKI（Public Key Infrastruct

ure）方式に従い、VPNクライアント装置（A）１０１の公開鍵証明書CERT_A、及び、VPNゲートウェイ装置（B）１０３の公開鍵証明書CERT_Bを認証する。また、アクセスコントロールリスト（ACL）は公開鍵PUBLICKEY_AとプライベートIPアドレスIPADDRESS_Cを関連付けたデータで、VPNゲートウェイ装置（B）１０３で保管される。また、秘密鍵PRIVATEKEY_Sは、仲介装置（S）１０６で保管される。CERT_Sは、秘密鍵PRIVATEKEY_Sと対となる公開鍵PUBLICKEY_Sを含むX. 509形式の公開鍵証明書で、認証局（CA）１０６の秘密鍵で署名され、仲介装置（S）１０４で保管される。

【００７０】

仲介装置（S）１０４は（１）VPNゲートウェイ装置（B）１０３の公開鍵PUBLICKEY_Bをドメインネームサーバ（DNS）１０５に提示して、VPNゲートウェイ装置（B）１０３に割り当てられたIPアドレスIPADDRESS_Bを取得する手段、（２）VPNゲートウェイ装置（B）１０３で保管されるアクセスコントロールリスト（ACL）を記憶する手段、（３）アクセスコントロールリスト（ACL）を参照してアクセス権限制御を実行する手段、及び、（４）共通鍵KEY_ABを生成する手段を具備している。上記（１）に示す手段は、DNS方式と呼ばれるインターネットにおける一般的な名前解決方式に従って、公開鍵PUBLICKEY_BからIPアドレスIPADDRESS_Bを解決する。また、上記（２）に示す手段は、公開鍵PUBLICKEY_Bと関連付けてアクセスコントロールリスト（ACL）を管理する。また、上記（３）に示す手段は、公開鍵証明書CERT_Aに含まれる公開鍵PUBLICKEY_Aをアクセスコントロールリスト ACLに提示して検索し、検索結果として、公開鍵PUBLICKEY_Aと一意に関連付けられたプライベートIPアドレスIPADDRESS_Cを出力する。また、上記（４）に示す手段は、VPNクライアント装置（A）１０１とVPNゲートウェイ装置（B）１０３との間のIKEフェーズ1における認証に用いる共通鍵KEY_ABを生成する。

【００７１】

次に、図１１を参照して、図１０の動作概要を説明する。

アクセスコントロールル（ACL)の登録(記憶)時、ＶＰＮゲートウェイ装置（B)１０３は、公開鍵PUBLICKEY_B（またはそのHASH-B)とアクセスコントロール(ＡＣＬ）を仲介装置（S)104に送信する(ステップ21)。仲介装置(Ｓ）は該公開鍵PUBLICKEY_B（またはそのHASH-B）と関連付けてアクセスコントロール（ACL)を記憶する。VPNゲートウェイ装置（B）103を経由して、VPNクライアント装置（A）101から通信装置（C）１１１にIPsecトンネルモードによるリモートアクセスVPNを実行する場合、VPNクライアント装置（A）101は、公開鍵PUBLICKEY_Ａと公開鍵PUBLICKEY_B（またはそのHASH-B）を仲介装置(S)104に送信して、VPNゲートウェイ装置（B）103及び通信装置(C)IPアドレスの検索要求を行なう(ステップ22)。

【００７２】

仲介装置(S)104は、PKI方式に従ってVPNクライアント装置(A)101のアクセス権限制御を実行し、アクセスを許可する場合には、ドメインネームサーバ(DNS)105を検索してVPNゲートウェイ装置（B）103に割り当てられたIPアドレスIPADDRESS_Bを取得する(ステップ23)。また、仲介(S)104は、アクセスコントロール(ACL)を参照して、VPNゲートウェイ装置（B）103により管理されるLAN110に接続された通信装置(C)111に割当てられたプライベートIPアドレスIPADDRESS_Cを取得する。さらに、仲介装置(S)104は、VPNクライアント装置（A）101との間の認証に用いる共通鍵KEY-ABを生成する。そして、仲介装置(S)104は、仲介装置(S)104とVPNクライアント装置（A）101との間の通信路を暗号化し、VPNクライアント装置（A）101へIPADDRESS_B、IPADDRESS_C及び共通鍵KEY_ABを送信する(ステップ24)。また、仲介装置(S)104は、仲介装置(S)104とVPNゲートウェイ装置（B）103との間の通信路を暗号化し、VPNゲートウェイ装置（B）103へIPADDRESS_AとKEY_ABを送信する(ステップ25)。

【００７３】

以上、図１０に示すシステムの各装置の構成及び全体の動作概要を述べたが、ドメインネームサーバ（DNS）１０５におけるIPアドレスの管理及び名前解決方法、及び、IPsecトランスポートモードまたはトンネルモードによる通信路の暗号化方法、共通鍵KEY_ABの生

成方法、及び、PKI方式によるX．509形式の公開鍵証明書CERT_A及びCERT_Bの認証方式については、当業者にとってよく知られているので、その詳細な構成は省略する。

【００７４】

以下に、本実施例２におけるアクセスコントロールリスト(ACL)の記憶手順、及びIPアドレスの取得、共通鍵の生成、これらIPアドレスと共通鍵の送信手順について詳述する。

【００７５】

まず、図１２及び図１３を参照して、VPNゲートウェイ装置(B)103において保管されるアクセスコントロールリスト(ACL)を仲介装置(S)104に記憶する手順について説明する。

図12において、VPNゲートウェイ装置(B)103と仲介装置(S)104は、IPsecトランスポートモードにより接続する(ステップ1301)。IKEフェーズ1における認証はPKI方式に従い、VPNゲートウェイ装置(B)103は公開鍵証明書CERT_Bを送信し、仲介装置(S)104は公開鍵証明書CERT_Sを送信する。VPNゲートウェイ装置(B)103は受信した公開鍵証明書CERT_Sを認証局(CA)106に問い合わせて、公開鍵証明書CERT_Sの正しさをPKI方式に従って認証する。同様に、仲介装置(S)104は受信した公開鍵証明書CERT_Bを認証局CAに問い合わせて、公開鍵証明書CERT_Bの正しさをPKI方式に従って認証する。

【００７６】

VPNゲートウェイ装置(B)103は、ステップ1301において暗号化された通信路を用いて、アクセスコントロールリスト(ACL)をすべて送信する(ステップ1302)。仲介装置(S)104は、VPNゲートウェイ装置（B）103から送信されたアクセスコントロールリスト(ACL)を登録する(ステップ１３０３)。その後、VPNゲートウェイ装置（B）103と仲介装置(S)104は、接続を切断する(ステップ１３０４)。

【００７７】

図１３は仲介装置(S)104でのアクセスコントロールリスト(ACL)の登録手順の詳細フローである。仲介装置(S)104は、まずVPNゲートウェイ装置（B）103から送信されたアクセスコントロールリスト(ACL)をすべて受信する(ステップ１４０１)。次に、先のステップ1301におけるIKE認証で用いた公開鍵証明書 CERT_Bを参照して、公開鍵PUBLICKEY_Bを取得する(ステップ１４０２)。次に、この取得した公開鍵PUBLICKEY_Bとステップ1401で受信したアクセスコントロールリストACLを関連づけて記憶する（ステップ１４０３)。

【００７８】

次に、図１４及び図１５を参照して、仲介装置(S)104が、VPNクライアント装置(A)101とVPNゲートウェイ装置(B)103との間の共通鍵KEY_ABを生成し、VPNゲートウェイ装置(B)103に割り当てられたIPアドレスIPADDRESS_B、通信装置(C)111に割り当てられたプライベートIPアドレスIPADDRESS_C、及び、共通鍵KEY_ABをVPNクライアント装置(A)101に送信し、また、VPNクライアント装置(A)101に割り当てられたIPアドレスIPADDRESS_A、及び、共通鍵KEY_ABをVPNゲートウェイ装置(B)103に送信する手順について説明する。

【００７９】

図１４において、VPNクライアント装置(A)101と仲介装置(S)104は、IPsecトランスポートモードにより接続する(ステップ１５０１)。IKEフェーズ1における認証はPKI方式に従い、VPN クライアント装置(A)101は公開鍵証明書CERT_Aを送信し、仲介装置(S)104は公開鍵証明書CERT_Sを送信する。VPNクライアント装置(A)101は受信した公開鍵証明書CERT_Sを認証局(CA)106に問い合わせて、公開鍵証明書CERT_Sの正しさをPKI方式に従って認証する。同様に、仲介装置(S)104は受信した公開鍵証明書CERT_Aを認証局(CA)106に問い合わせて、公開鍵証明書CERT_Aの正しさをPKI方式に従って認証する。

【００８０】

VPNクライアント装置(A)101は、ステップ１５０１において暗号化された通信路を用いて、VPNゲートウェイ装置(B)103の公開鍵PUBLICKEY_Bを含むDNSクエリQUERYをすべて送信する(ステップ１５０２)。仲介装置(S)104は、VPNクライアント装置（A）101に割り当てられたIPアドレスIPADDRESS_A、VPNゲートウェイ装置（B）103に割り当てられたIPアドレスにIPアドレスIPADDRESS_B、VPNゲートウェイ装置（B）103により管理されるLAN110に接続される通信装置(C)111に割り当てられたプライベートIPアドレスIPADDRESS_Cを取得し

、VPNクライアント装置（A）101とVPNゲートウェイ装置（B）103との間のIKE等の認証に用いる共通鍵KEY-ABを生成する(ステップ１５０３)。図１５はステップ１５０３の詳細処理フローである。

【００８１】

図１５において、仲介装置(S)104は、まず、VPNクライアント装置（A）101から送信されたDNSクエリQUERYをすべて受信して入力する(ステップ１６０１)。次に、入力したDNSクエリQUERYを参照して、公開鍵PUBLICKEY_Bをすべて取得する(ステップ１６０２)。次に、取得した公開鍵PUBLICKEY_Bをもとに、それに関連付けられたアクセスコントロールリスト（ACL）をすべて取得する(ステップ６３)。次に、先のステップ１５０１におけるIKEフェーズ1認証に用いた公開鍵証明書CERT_Aを参照して、公開鍵PUBLICKEY_Aをすべて取得する(ステップ１６０４)。次に、この取得した公開鍵PUBLICKEY_Aをもとにアクセスコントロールリスト(ACL)を検索し、プライベートIPアドレスIPADDRESS_Cを取得する(ステップ１６０５)。そして、プライベートIPアドレスIPADDRESS_Cが取得されたと判定し(ステップ１６０６)、いかなるIPアドレスも取得できない場合には終了する。

【００８２】

プライベートIPアドレスIPADDRESS_Cが取得されたなら、次に、仲介装置Sは、上記ステップ１６０１において受信したDNSクエリQUERYをドメインネームサーバ(DNS)105に提示して、IPアドレスIPADDRSSS_Bを取得する(ステップ１６０７)。
VPNクライアント装置AのIPアドレスIPADDRESS_Aを取得する(ステップ１６０８)。共通鍵KEY_ABを生成する(ステップ１６０９)。

【００８３】

図１４に戻り、仲介装置(S)104は、ステップ１５０１おいて暗号化された通信路を用いて、ステップ１６０７で取得したIPアドレスIPADDRESS_B、ステップ１６０５で取得したプライベートIPアドレスIPADDRESS_C、及び、ステップ１６０９で生成した共通鍵KEY-ABをすべてVPNクライアント装置(A)1609に送信する(ステップ１５０４)。次に、VPNクライアント装置(A)101と仲介装置(S)104は、接続を切断する(ステップ１５０５)。

【００８４】

次に、VPNゲートウェイ装置（B）103と仲介装置(S)104は、IPsecトランスポートモードにより接続する(ステップ1506)。IKEフェーズ1における認証はPKI方式に従い、VPN ゲートウェイ装置(B)103は公開鍵証明書CERT_Bを送信し、仲介装置Sは公開鍵証明書CERT_Sを送信する。VPNゲートウェイ装置(B)103は、受信した公開鍵証明書CERT_Sを認証局(CA)106に問い合わせて、公開鍵証明書CERT_Sの正しさをPKI方式に従って認証する。同様に、仲介装置(S)104は、受信した公開鍵証明書CERT_Bを認証局(CA)106に問い合わせて、公開鍵証明書CERT_Bの正しさをPKI方式に従って認証する。

【００８５】

仲介装置(S)104は、ステップ１５０６において暗号化された通信路を用いて、先のステップ１６０８において取得したIPアドレスIPADDRESS_A、及び、先のステップ１６０９において生成した共通鍵KEY_ABをすべてVPNゲートウェイ装置(B)103に送信する(ステップ１５０７)。VPNゲートウェイ装置(B)103と仲介装置(S)104は、接続を切断する(ステップ１５０８)。

【００８６】

以上述べたように、本実施例において、仲介装置(S)104は、VPNゲートウェイ装置(B)103より送信された、通信装置(C)111に割り当てられたプライベートIPアドレスIPADDRESS_Cを記憶することで、仲介装置(S)104は、VPNゲートウェイ装置(B)103だけが知っている、ローカルエリアネットワーク(LAN)に接続された通信装置(C)111に割り当てられたプライベートIPアドレスIPADDRESS_Cを知ることができる。従って、VPNクライアント装置(A)101は、VPNゲートウェイ装置(B)103を介した通信装置(C)111へのIPsecトンネルモードによるリモートアクセスVPNに必要なプライベートIPアドレスIPADDRESS_Cを、リモートアクセスVPNを実行する前に仲介装置(S)104に問い合わせることにより知ることができる。

【００８７】

また、本実施例において、仲介装置(S)104は、共通鍵KEY_ABを生成し、生成した共通鍵KEY_ABをVPNクライアント装置(A)101とVPNゲートウェイ装置(B)103の両者に送信するこれによって、VPNクライアント装置(A)101とVPNゲートウェイ装置(B)103はともに共通鍵KEY_ABを受信できる。従って、VPNクライアント装置(A)101とVPNゲートウェイ装置(B)103はIKEフェーズ1における認証に用いる共通鍵KEY_ABをオンラインで共有できる。

【００８８】

また、本実施例において、仲介装置(S)104は、VPNゲートウェイ装置(B)103を認証し、認証に成功した場合に限り、VPNゲートウェイ装置(B)103より送信された、通信装置(C)111に割り当てられたプライベートIPアドレスIPADDRESS_Cを、仲介装置(S)104に記憶する。これによって、仲介装置(S)104は、偽装されていないVPNゲートウェイ装置(B)103から送信されたプライベートIPアドレスIPADDRESS_Cに限り記憶できる。従って、VPNクライアント装置(A)101は、正しいVPNゲートウェイ装置(B)103から送信されたプライベートIPアドレスIPADDRESS_Cを知ることができる。

【００８９】

また、本実施例において、仲介装置(S)104は、VPNゲートウェイ装置(B)103を認証し、認証に成功した場合に限り、VPNゲートウェイ装置(B)103より送信された、通信装置(C)101に割り当てられたプライベートIPアドレスIPADDRESS_Cを、仲介装置(S)104に記憶するという動作において、仲介装置(S)104とVPNゲートウェイ装置(B)103との間の通信を暗号化する。これによって、仲介装置(S)104は、VPNゲートウェイ装置(B)103から送信された、通信装置(C)111に割り当てられたプライベートIPアドレスIPADDRESS_Cを改ざんされることなく、かつ、盗聴されることなく受信できる。従って、VPNクライアント装置(A)101は、正しいVPNゲートウェイ装置(B)103から送信された、通信装置(C)111に割り当てられた正しいプライベートIPアドレスIPADDRESS_Cを知ることができるという効果が得られる。また、VPNゲートウェイ装置(B)103は、通信装置(C)111に割り当てられた正しいプライベートIPアドレスIPADDRESS_Cを不特定多数に知られることなく仲介装置(S)104に送信できる。

【００９０】

また、本実施例において、仲介装置(S)104は、VPNクライアント装置(A)101を認証し、認証に成功した場合に限り、VPNゲートウェイ装置(B)103に割り当てられたIPアドレスIPADDRESS_Bをドメインネームサーバ(DNS)105に問い合わせて取得し、共通鍵KEY_ABを生成し、取得したIPアドレスIPADDRESS_B、通信装置(C)111に割り当てられたIPアドレスIPADDRESS_B、及び、生成した共通鍵KEY_ABをすべてVPNクライアント装置(A)101に送信する。これによって、仲介装置(S)104は、VPNクライアント装置(A)101が偽装されていない場合に限り、VPNゲートウェイ装置(B)103に割り当てられたIPアドレスIPADDRESS_B、通信装置(C)111に割り当てられたプライベートIPアドレスIPADDRESS_C、及び、共通鍵KEY_ABのすべてをVPNクライアント装置(A)101に送信できる。従って、正しいVPNクライアント装置(A)101に限り、VPNゲートウェイ装置(B)103を介して、通信装置(C)111とIPsecトンネルモードによるリモートアクセスVPNを実行できる。

【００９１】

また、本実施例において、仲介装置(S)104は、VPNクライアント装置(A)101がVPNゲートウェイ装置(B)103に割り当てられたIPアドレスIPADDRESS_Bを検索する権限を有しているか否かを判定し、権限を有している場合に限り、VPNゲートウェイ装置Bに割り当てられたIPアドレスIPADDRESS_Bをドメインネームサーバ(DNS)105に問い合わせて取得し、共通鍵KEY_ABを生成し、取得したIPアドレスIPADDRESS_B、通信装置(C)111に割り当てられたIPアドレスIPADDRESS_B、及び、生成した共通鍵KEY_ABをすべてVPNクライアント装置(A)101に送信する。これによって、仲介装置(S)104は、VPNゲートウェイ装置(B)101に割り当てられたIPアドレスIPADDRESS_B、通信装置(C)111に割り当てられたプライベートIPアドレスIPADDRESS_C、及び、共通鍵KEY_ABのすべてを、VPNゲートウェイ装置(B)103、及び、通信装置(C)111に対しあらかじめアクセス権限を有するVPNクライアント装置(A)101だけに送信できる。従って、VPNゲートウェイ装置(B)103、及び、通信装置(C)111に対する、不特

定多数からのIPsecトンネルモードによるリモートアクセスVPNを防止できる。

【００９２】

また、本実施例において、仲介装置(S)104は、仲介装置(S)104とVPNクライアント装置(A)101との間の通信を暗号化する。これによって、仲介装置(S)104は、VPNゲートウェイ装置(B)103に割り当てられたIPアドレスIPADDRESS_B、通信装置(C)111に割り当てられたプライベートIPアドレスIPADDRESS_C、及び、共通鍵KEY_ABを改ざんされることなく、かつ、盗聴されることなくVPNクライアント装置(A)に送信できる。従って、VPNクライアント装置(A)101は、正しいVPNゲートウェイ装置(B)103を介して、正しい通信装置(C)111と、IPsecトンネルモードによるリモートアクセスVPNを実行できる。

【００９３】

また、本実施例において、仲介装置(S)104は、VPNゲートウェイ装置(B)103を認証し、認証に成功した場合に限り、VPNクライアント装置(A)101に割り当てられたIPアドレスIPADDRESS_A、及び、共通鍵KEY_ABをVPNゲートウェイ装置(B)103に送信する。これによって、仲介装置(S)104は、VPNゲートウェイ装置(B)103が偽装されていない場合に限り、VPNクライアント装置(A)101に割り当てられたIPアドレスIPADDRESS_A、及び、共通鍵KEY_ABをVPNゲートウェイ装置(B)103に送信できる。従って、VPNクライアント装置Aは、正しいVPNゲートウェイ装置(B)103を介して、通信装置(C)111とIPsecトンネルモードによるリモートアクセスVPNを実行できる。

【００９４】

また、本実施例において、仲介装置(S)104は、VPNゲートウェイ装置(B)103を認証し、認証に成功した場合に限り、VPNクライアント装置(A)101に割り当てられたIPアドレスIPADDRESS_A、及び、共通鍵KEY_ABをVPNゲートウェイ装置(B)103に送信するという動作において、仲介装置(S)104とVPNゲートウェイ装置(B)103との間の通信を暗号化する。これによって、仲介装置(S)104は、VPNクライアント装置(A)101に割り当てられたIPアドレスIPADDRESS_A、及び、共通鍵KEY_ABをすべて改ざんされることなく、かつ、盗聴されることなくVPNゲートウェイ装置(B)103に送信できる。従って、VPNゲートウェイ装置(B)103、及び、通信装置(C)111は、正しいVPNクライアント装置(A)101と、IPsecトンネルモードによるリモートアクセスVPNを実行できる。

【００９５】

また、本実施例において、仲介装置(S)104は、PKI方式に従って、VPNクライアント装置(A)101、及び、VPNゲートウェイ装置(B)103を認証する。これによって、VPNクライアント装置(A)101の公開鍵証明書CERT_AもVPNゲートウェイ装置(B)103の公開鍵証明書CERT_Bも仲介装置(S)104に送信することにより認証できる。従って、VPNクライアント装置(A)101の個人情報をVPNゲートウェイ装置(B)103に対して隠蔽できる。同様に、VPNゲートウェイ装置(B)103の個人情報をVPNクライアント装置(A)101に対して隠蔽できる。

なお、本実施例における図10、図11に示すドメインネームサーバ(DNS)105において、公開鍵PUBLICKEY_Bの任意のハッシュ演算アルゴリズムによるハッシュ値HASH_Bと IPADDRESS_Bを関連付けて管理する場合、VPNゲートウェイ装置(B)102は公開鍵PUBLICKEY_Bのハッシュ値HASH_Bを生成してから、ハッシュ値HASH_BとIPアドレスIPADDRESS_Bをドメインネームサーバ(DNS)105に登録すればよい。また、図14に示す手順のステップ1502を、公開鍵PUBLICKEY_Bの任意のハッシュ演算アルゴリズムによるハッシュ値HASH_Bを含むDNSクエリQUERYに変更することにより明らかに実施できる。

【００９６】

また、アクセスコントロールリスト(ACL)において、公開鍵PUBLICKEY_AとIPアドレスIPADDRESS_Cを関連付けて管理する代わりに、公開鍵PUBLICKEY_Aの任意のハッシュ演算アルゴリズムによるハッシュ値HASH_AとIPアドレスIPADDRESS_Cと関連付けて管理しても良い、本変更に伴い、図１２に示す手順のステップ1302において、VPNゲートウェイ装置(B)103は公開鍵PUBLICKEY_Aのハッシュ値HASH_Aを生成してから、ハッシュ値HASH_AとIPアドレスIPADDRESS_Cをアクセスコントロールリスト(ACL)として関連付けたデータを送信することにより明らかに実施できる。かつ、図１５に示す手順のステップ1605を公開鍵PUBLICKE

Y_Aのハッシュ値HASH_Aを生成し、ハッシュ値HASH_Aを提示してアクセスコントロールリストACLを検索する手順に変更することにより、明らかに実施できる。

【００９７】

また、VPNクライアント装置(A)101にはグローバルIPアドレスIPADDRESS_Aのみを割り当てているが、これに加えて、仲介装置(S)104において、非特許文献1に示す方法等を用いてローカルエリアネットワークLAN内の任意のプライベートIPアドレスを割り当てても良い。

【００９８】

なお、実施例１や実施例２で示したシステムにおける各装置の一部もしくは全部の処理機能をコンピュータのプログラムで構成し、そのプログラムをコンピュータを用いて実行して本発明を実現することができること、あるいは、実施例１や実施例２で示した処理手順をコンピュータのプログラムで構成し、そのプログラムをコンピュータに実行させることができることは言うまでもない。コンピュータでその処理機能を実現するためのプログラム、あるいは、コンピュータにその処理手順を実行させるためのプログラムを、そのコンピュータが読み取り可能な記録媒体、例えば、ＦＤ、ＭＯ、ＲＯＭ、メモリカード、ＣＤ、ＤＶＤ、リムーバブルディスクなどに記録して、保存したり、提供したりすることができるとともに、インターネット等のネットワークを通してそのプログラムを配布したりすることが可能である。

【図面の簡単な説明】

【００９９】

【図１】本発明の第１の実施例におけるシステム構成例を示す図である。

【図２】本発明の第１の実施例の動作概要を説明する図である。

【図３】本発明の第１の実施例におけるアクセスコントロールACLの記憶手段を示す図である。

【図４】本発明の第１の実施形態におけるIPアドレス及び共通鍵の送信手順を示す図である。

【図５】本発明の第１の実施例における仲介装置でのIPアドレスの取得手順、及び、共通鍵の生成手順の詳細処理フロー図である。

【図６】本発明の第１の実施例におけるアクセスコントロールリストACLの一例である。

【図７】本発明の第１の実施例におけるデータTAGの一例である。

【図８】本発明の第１の実施例における演算結果データDATAの一例である。

【図９】本発明の第１の実施例における証明書CERTの一例である。ットワークを通してそのプログラムを配布したりすることが可能である。

【図１０】本発明の第２の実施例におけるシステム構成例を示す図である。

【図１１】本発明の第２の実施例の動作概要を説明する図である。

【図１２】本発明の第２の実施例におけるアクセスコントロールACLの記憶手段を示す図である。

【図１３】本発明の第２の実施例における仲介装置でのアクセスコントロールリストACLの記憶手順の詳細処理フロー図である。

【図１４】本発明の第２の実施例におけるIPアドレス及び共通鍵の配布手順を示す図である。

【図１５】本発明の第２の実施例における、仲介装置でのIPアドレスの取得手順、及び、共通鍵の生成手順の詳細処理フロー図である。

【符号の説明】

【０１００】

１００　IPネットワーク（WAN）

１０１，１０２　VPNクライアント装置

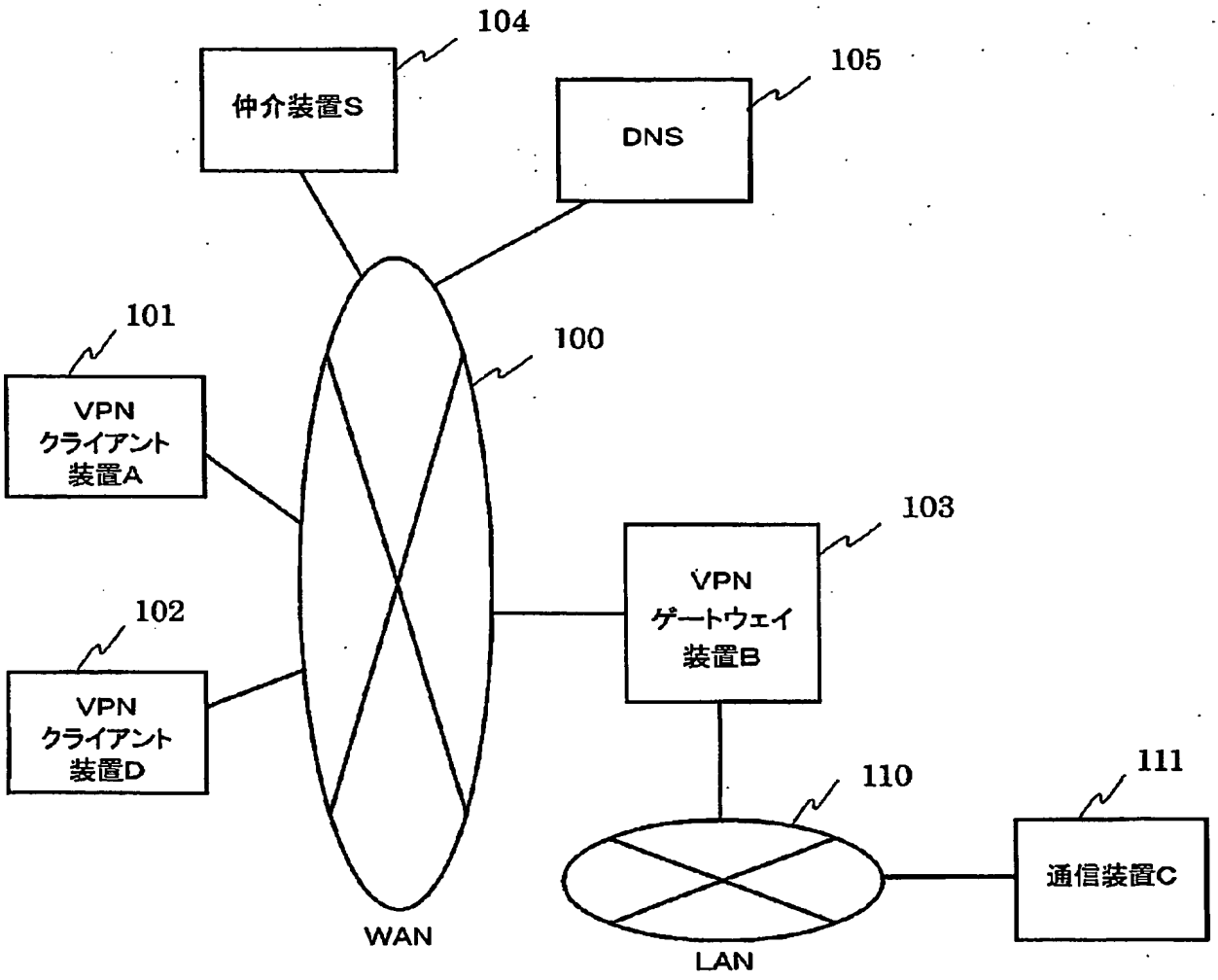
１０３　VPNゲートウェイ装置

１０４　仲介装置

１０５　ドメインネームサーバ（DNS）
１１０　ローカルエリアネットワーク（LAN）
１１１　通信装置

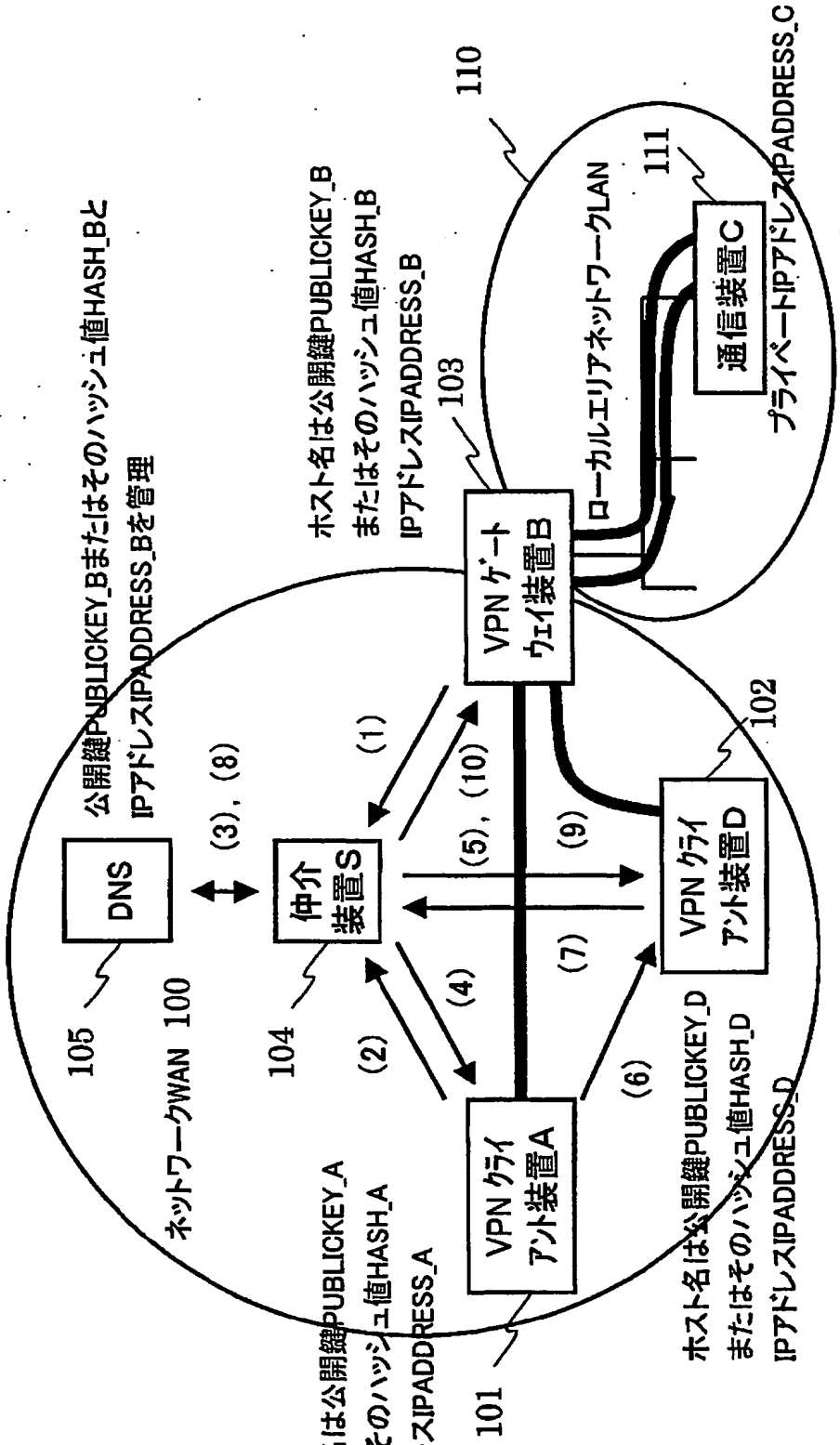
【書類名】図面
【図１】

本発明の第1の実施例のシステム構成例



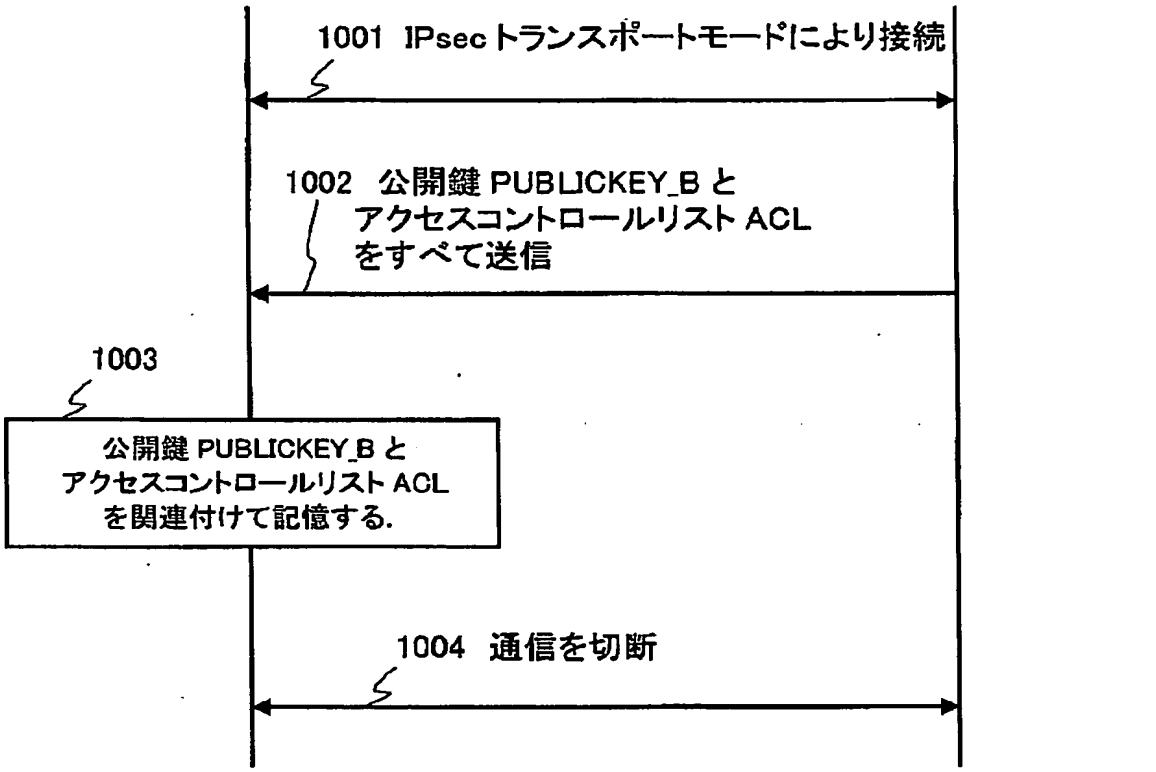
【図２】

本発明の第1の実施例の動作概要

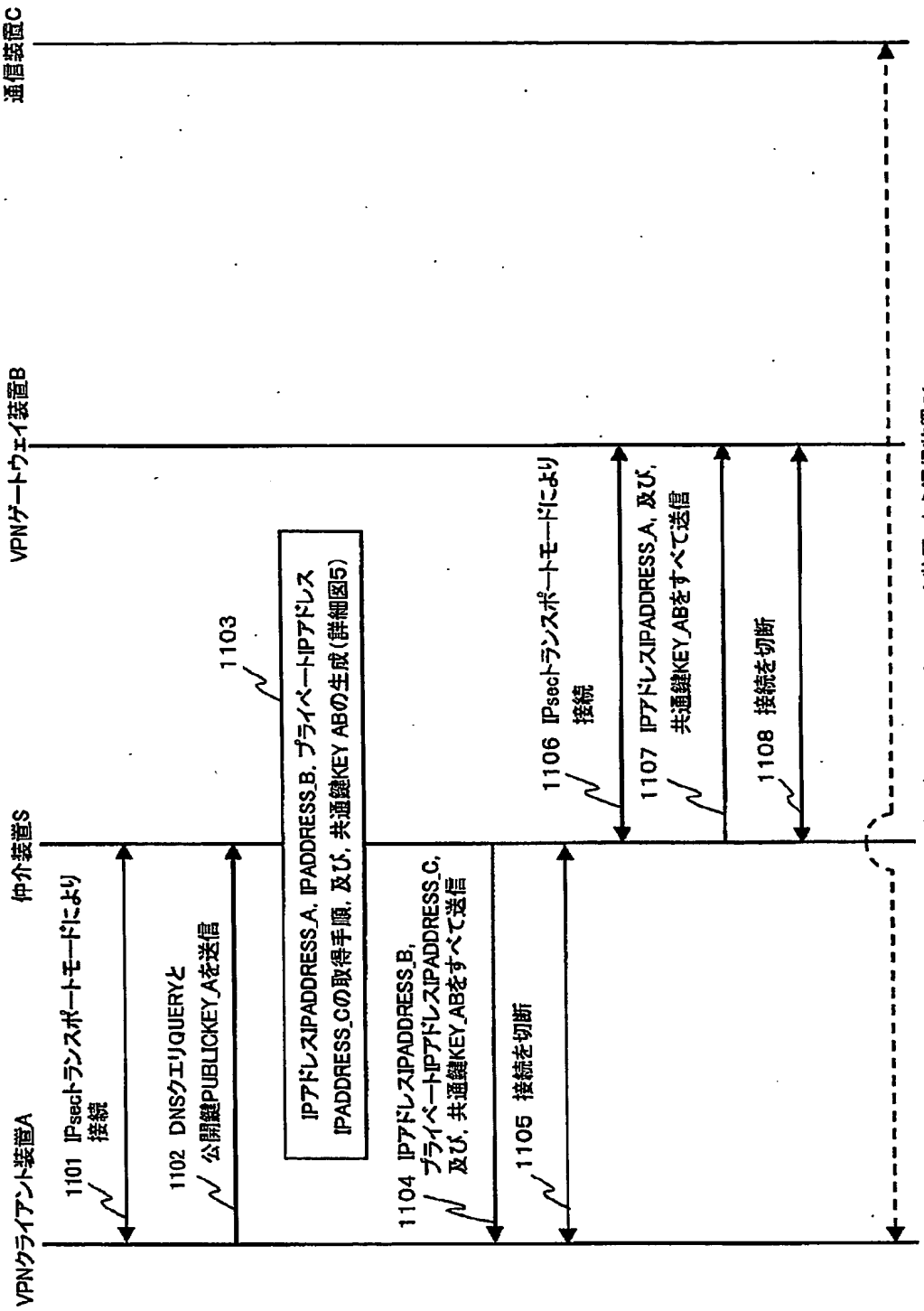


【図３】

本発明の第1の実施例におけるアクセスコントロールリストACLの記憶手順

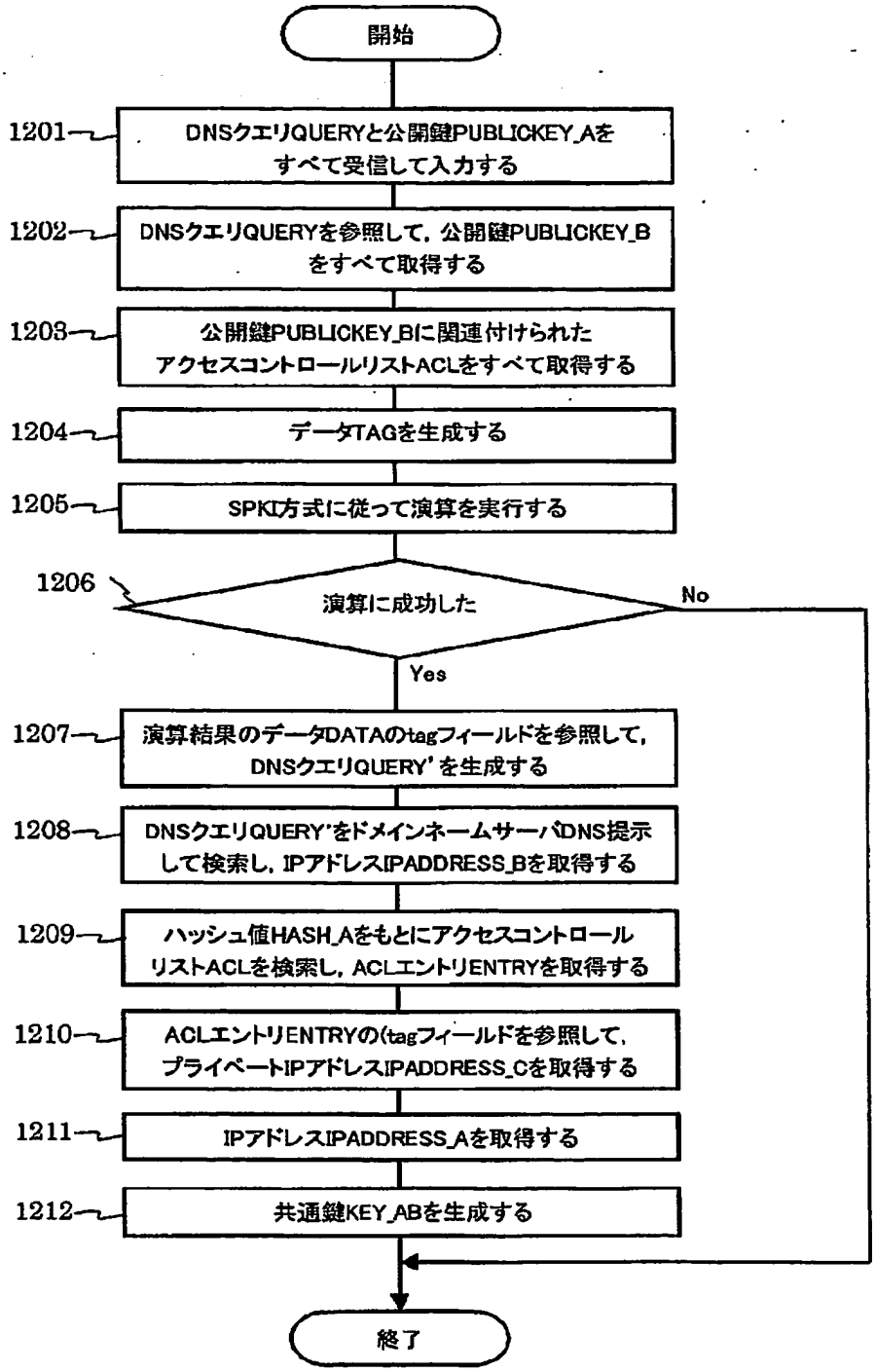


【図４】

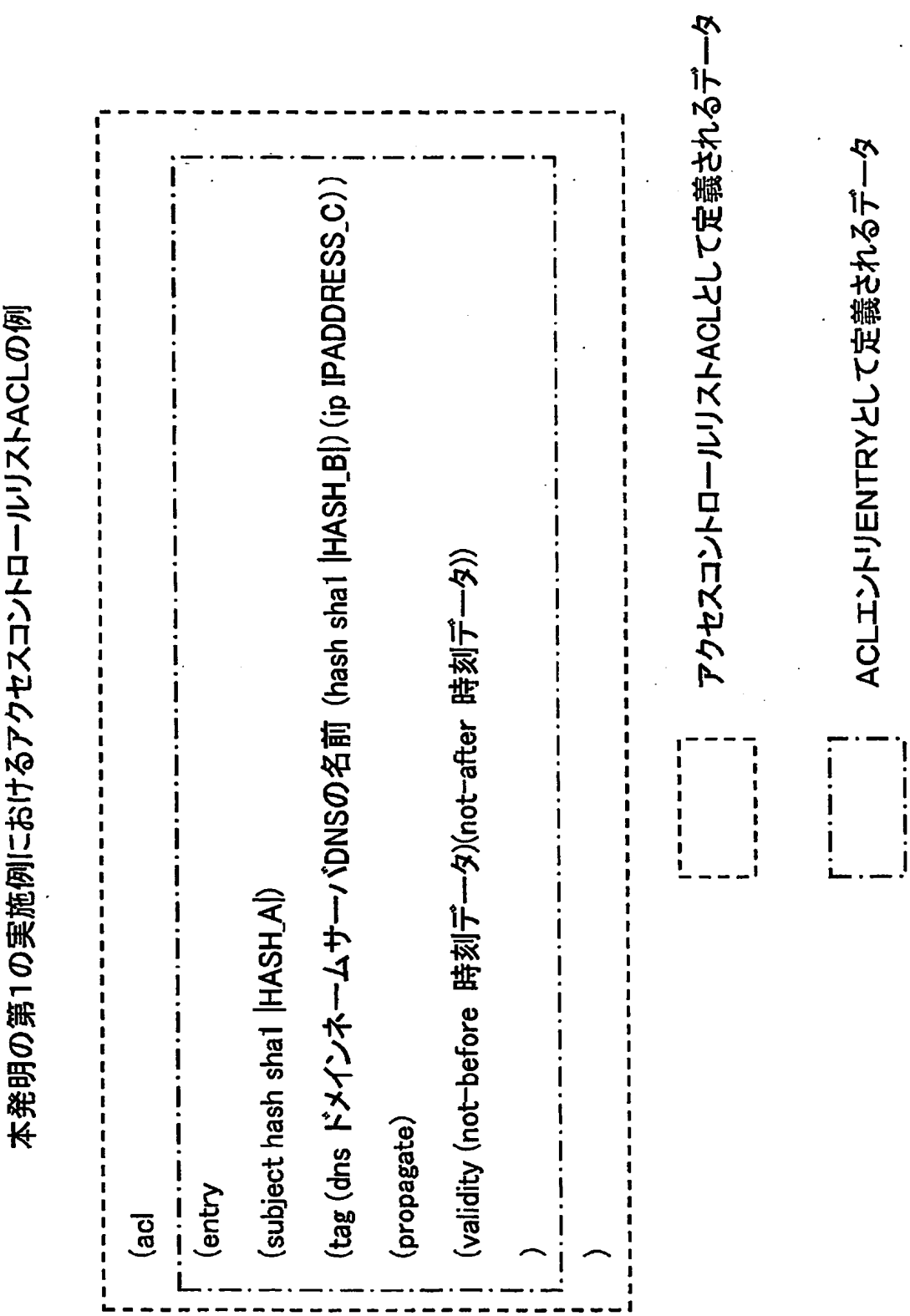

本発明の第1の実施例におけるIPアドレスIPADRESS_A, IPアドレスIPADRESS_B,
プライベートIPアドレスIPADRESS_C、および共通鍵KEY_AB送信手順
VPNクライアント装置A
仲介装置S
VPNゲートウェイ装置B
通信装置C
1101 IPsecトランスポートモードにより
接続
1102 DNSクエリQUERYと
公開鍵PUBLICKEY_Aを送信
1103
IPアドレスIPADDRESS_A, IPADDRESS_B, プライベートIPアドレス
IPADDRESS_Cの取得手順, 及び, 共通鍵KEY ABの生成(詳細図5)
1104 IPアドレスIPADDRESS_B,
プライベートIPアドレスIPADDRESS_C,
及び, 共通鍵KEY_ABをすべて送信
1105 接続を切断
1106 IPsecトランスポートモードにより
接続
1107 IPアドレスIPADDRESS_A, 及び,
共通鍵KEY_ABをすべて送信
1108 接続を切断
VPNゲートウェイ装置Bを経由して, VPNクライアント装置Aから通信装置Cに
IPsecトンネルモードによるリモートアクセスVPNを実行

【図５】

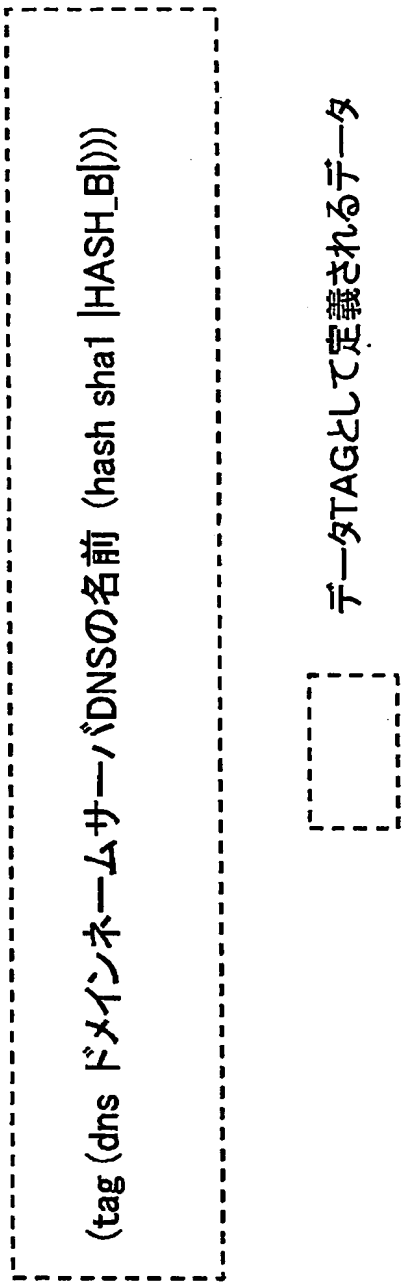
本発明の第１の実施例における IP アドレス IPADRESS_A, IP アドレス IPADRESS_B, プライベート IP アドレス IPADRESS_C、の取得手順、および共通鍵 KEY_AB の生成手順



【図６】


本発明の第１の実施例におけるアクセスコントロールリストACLの例
(acl
(entry
(subject hash sha1 |HASH_A|)
(tag (dns ドメインネームサーバDNSの名前 (hash sha1 |HASH_B|) (ip IPADDRESS_C))
(propagate)
(validity (not-before 時刻データ)(not-after 時刻データ))
)
)
アクセスコントロールリストACLとして定義されるデータ
ACLエントリENTRYとして定義されるデータ

【図７】


本発明の第１の実施例におけるデータTAGの例
(tag (dns ドメインネームサーバDNSの名前 (hash sha1 |HASH_B|)))
データTAGとして定義されるデータ

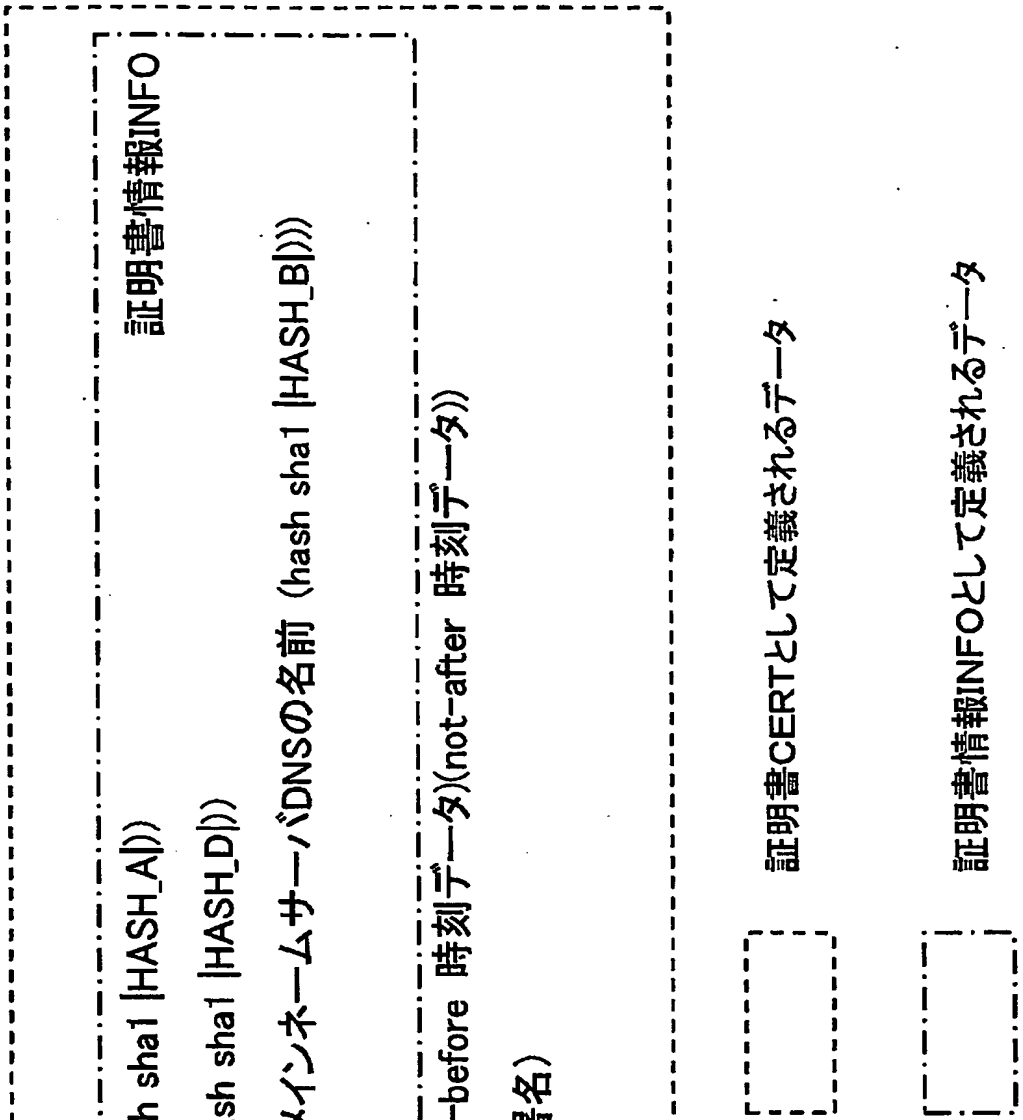
【図８】

本発明の第１の実施例における演算結果データDATAの例

```
(cert
(issuer Self)
(subject (hash sha1 |HASH_A|))
(tag (dns ドメインネームサーバDNSの名前 (hash sha1 |HASH_B|)))
(propagate)
(validity (not-before 時刻データ)(not-after 時刻データ))
)
```

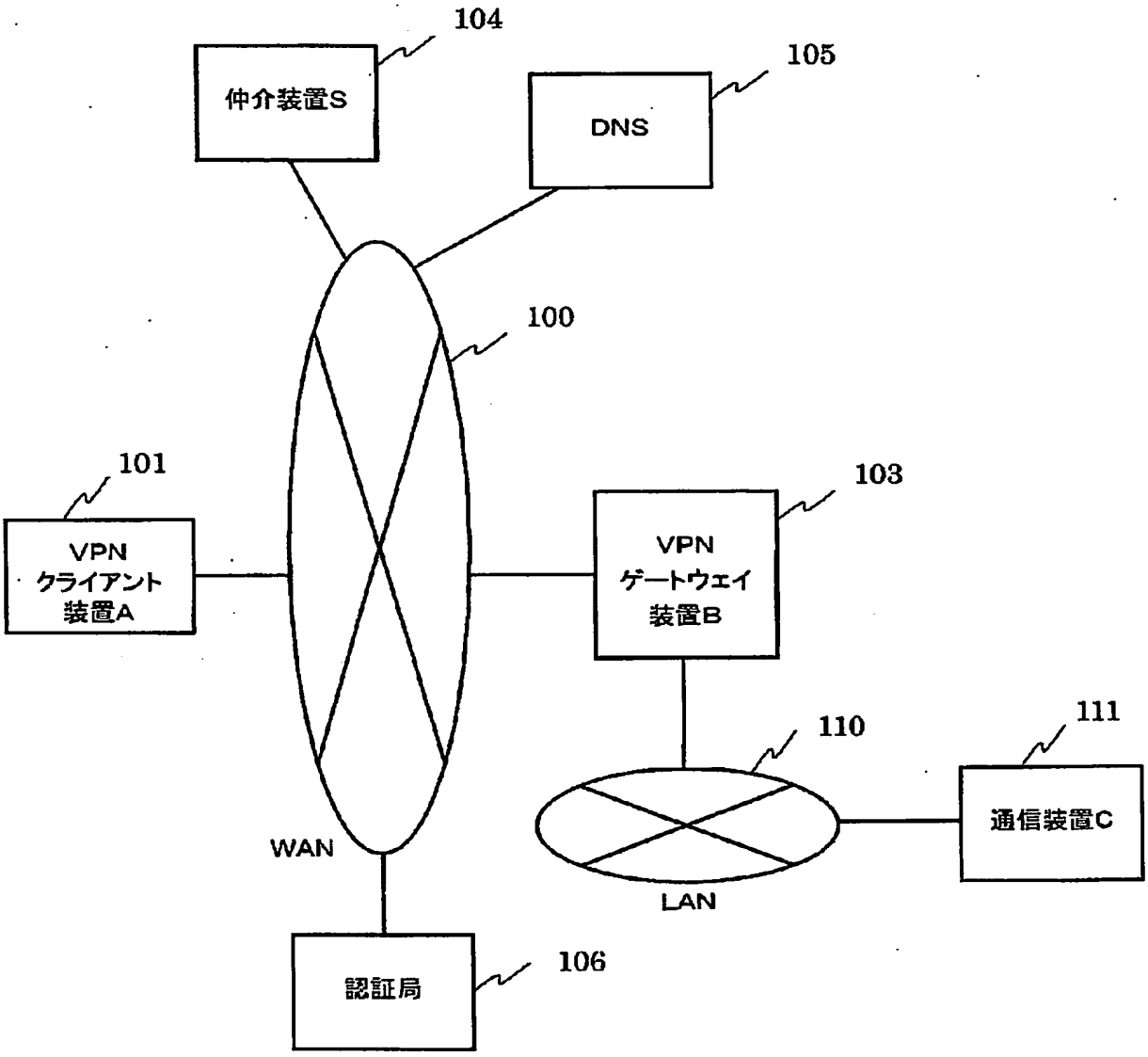
演算結果データDATAとして定義されるデータ

【図９】


本発明の第1の実施例における証明書CERTの例
(cert
(issuer (hash sha1 |HASH_A|))
(subject (hash sha1 |HASH_D|))
(tag (dns ドメインネームサーバDNSの名前 (hash sha1 |HASH_B|)))
(propagate)
(validity (not-before 時刻データ)(not-after 時刻データ))
(signature 署名)
)
証明書情報INFO
証明書CERTとして定義されるデータ
証明書情報INFOとして定義されるデータ

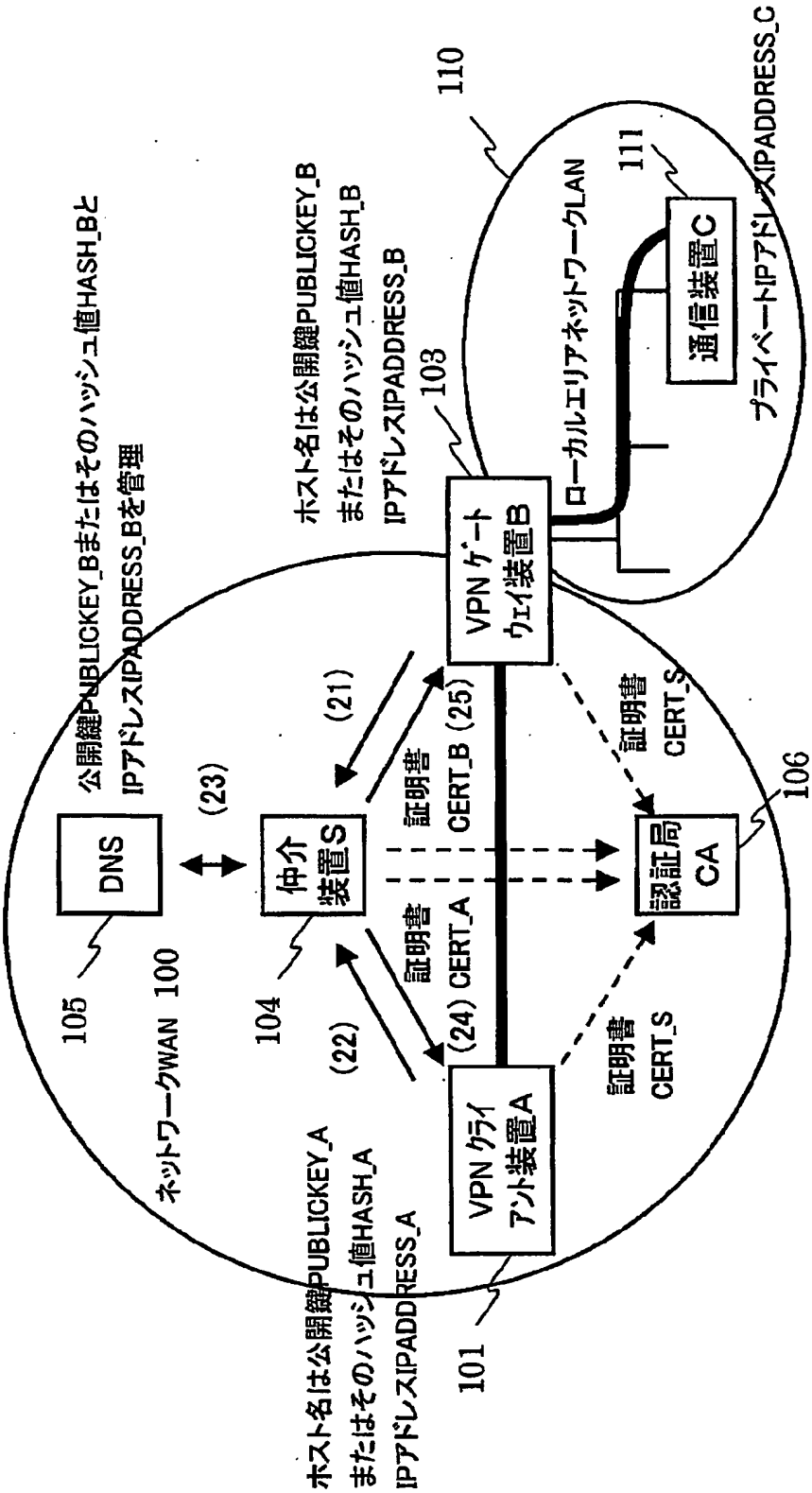
【図１０】

本発明の第2の実施例のシステム構成例



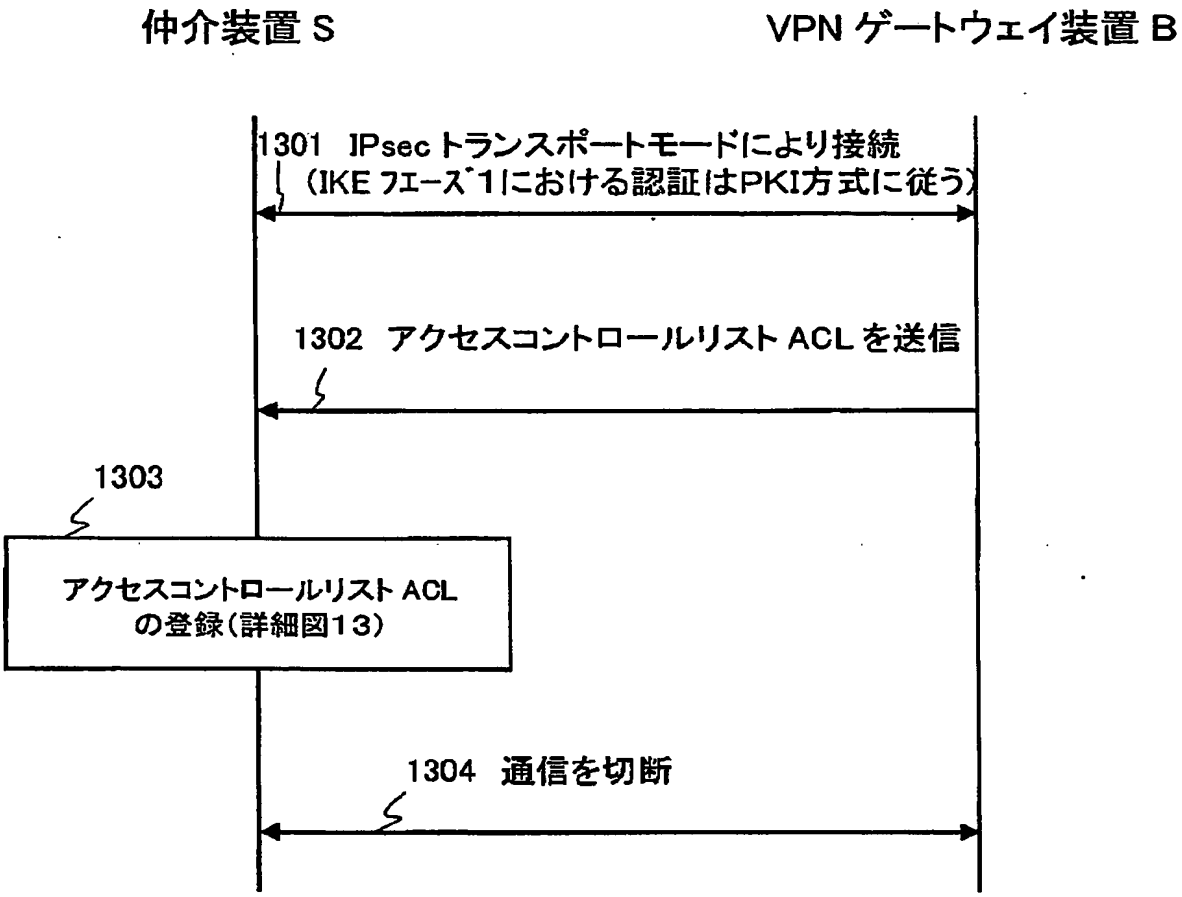
【図１１】

本発明の第2の実施例の動作概要



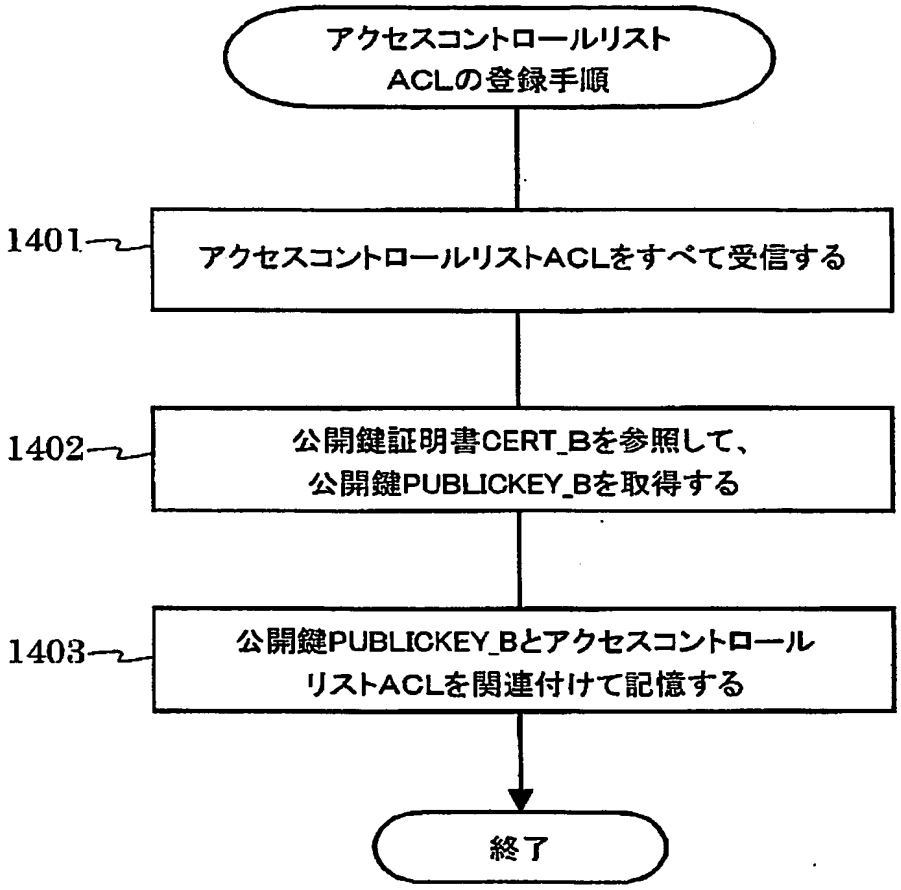
【図１２】

本発明の第2の実施例におけるアクセスコントロールリストACLの記憶手順

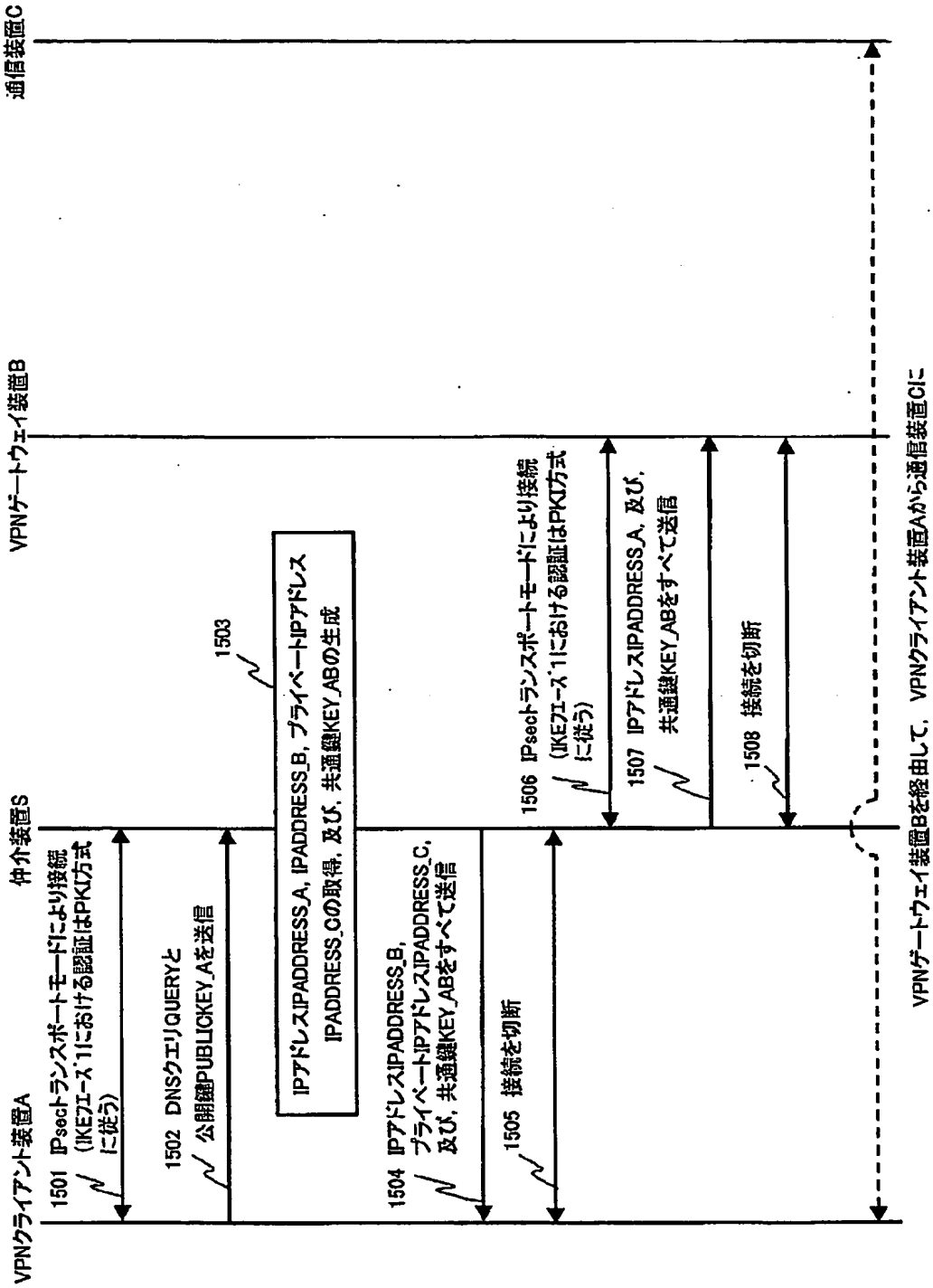


【図１３】

本発明の第2の実施例における仲介装置Sにおける
アクセスコントロールリストACLの記憶手順

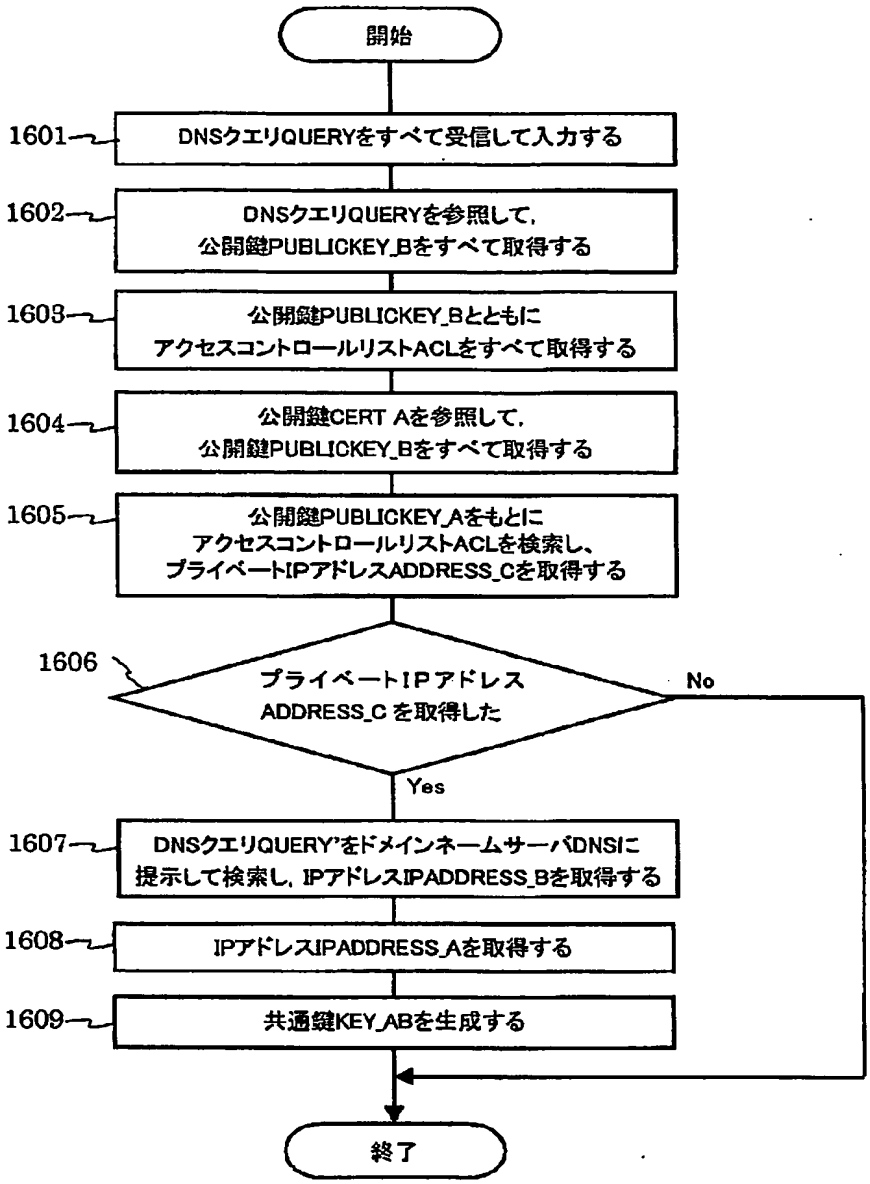


【図１４】


本発明の第2の実施例における IP アドレス IPADRESS_A, IP アドレス IPADRESS_B,
プライベート IP アドレス IPADRESS_C、および共通鍵 KEY_AB 送信手順
VPNクライアント装置A
仲介装置S
VPNゲートウェイ装置B
通信装置C
1501 IPsecトランスポートモードにより接続
(IKEフェーズ1における認証はPKI方式に従う)
1502 DNSクエリQUERYと
公開鍵PUBLICKEY_Aを送信
1503
IPアドレスIPADDRESS_A, IPADDRESS_B, プライベートIPアドレス
IPADDRESS_Cの取得, 及び, 共通鍵KEY_ABの生成
1504 IPアドレスIPADDRESS_B,
プライベートIPアドレスIPADDRESS_C,
及び, 共通鍵KEY_ABをすべて送信
1505 接続を切断
1506 IPsecトランスポートモードにより接続
(IKEフェーズ1における認証はPKI方式に従う)
1507 IPアドレスIPADDRESS_A, 及び,
共通鍵KEY_ABをすべて送信
1508 接続を切断
VPNゲートウェイ装置Bを経由して、VPNクライアント装置Aから通信装置Cに
IPsecトンネルモードによるリモートアクセスVPNを実行

【図１５】

本発明の第２の実施例におけるIPアドレスIPADRESS_A，IPアドレスIPADRESS_B，プライベートIPアドレスIPADRESS_C、の取得手順、および共通鍵KEY_ABの生成手順



【書類名】要約書
【要約】
【課題】　インターネットにおいて、ＩＰsec等のトンネリングプロトコルによるリモートアクセスＶＰＮを確立するための情報を安全に共有できるようにする。
【解決手段】　ＩＰネットワーク上に仲介装置を設け、ＶＰＮゲートウェイ装置で保管されるアクセスコントロールリスト（ＡＣＬ）を記憶する。仲介装置は、ＶＰＮクライアント装置から検索要求を受信し、ＡＣＬを参照して通信装置のプライベートＩＰアドレスを取得し、ＤＮＳを検索してＶＰＮゲートウェイ装置のＩＰアドレスを取得し、ＶＰＮクライアント装置とＶＰＮゲートウェイ装置との間の認証に用いる共通鍵を生成し、ＶＰＮゲートウェイ装置のＩＰアドレス、通信装置のプライベートＩＰアドレス及び共通鍵をＶＰＮクライアント装置に送信し、ＶＰＮクライアント装置のＩＰアドレス及び共通鍵をＶＰＮゲートウェイ装置に送信する。
【選択図】　図２

特願２００３－２７１２０２

出願人履歴情報

識別番号　［０００００４２２６］

１．変更年月日　１９９９年　７月１５日
［変更理由］　住所変更
住　所　東京都千代田区大手町二丁目３番１号
氏　名　日本電信電話株式会社